
تجارب شخصية مع الفيروسات
مشاكلها و حلولها
(الجزء الثاني)
bitdefender
eset
AVIR
لكاتبه
فهد سعيد مقرم

أعوذ بالله السميع العليم من الشيطان الرجيم

وما أوتيتم من العلم إلا قليلا

صدق الله العظيم

إهداء

إلى الغاليين والدايّ و إخوتي
إلى جميع المسلمين في كل مكان و زمان
إلى كل طالب معرفة في هذا المجال الحاسوبي الواسع
أهدي هذا الجهد المتواضع

الفهرس

نبذة عن كاتب الموضوع

الاســــــــــــم : فهد سعيد حيمد مقرم
تاريـــخ المـــيلاد : 27- 07- 1983
الديانـــــــــــة : مسلم لله الحمد و المنة
الجنسيــــــــــة : يمني من منطقة حضرموت شبام - قرية الحزم و أعيش بالسعودية - جدة
الدرجة العلميـــة : بكالريوس في علوم الحاسوب من جامعة حضرموت للعلوم و التكنولوجيا
الهوايـــــــات : كل ما يتعلق بالحاسوب من برامج و حماية و تصميم و غيرها
الحالة الاجتماعية : عازب ربنا ييسر بنت الحلال
الوظيفـــــــــة : بالانتظار أسأل الله الرزق الحلال
اسمي بالمنتـــدى : MaskFD
البريد الالكتروني : Maskfd77@hotmail.com



المقدمة

بسم الله الرحمن الرحيم

الحمد لله . . والصلاة والسلام على خير خلق الله . . وعلى آله وصحبه ومن تبع هداه

قبل البداية في الموضوع

هذا الموضوع هو الجزء الثاني وكتبته بمنتدى المشاغب بتاريخ (10-07-2009) و قمت هنا بتحويله لكتاب بصيغة PDF بتاريخ (11-08-2009) للنشر والتوزيع للفائدة العامة .. و أعتذر منكم على القصور في ترتيبه و تنسيقه لضيق وقتي .. أرجو لكم الفائدة والمتعة ..

ملاحظة

قد أقوم بإهمال بعض النقاط لأنه تم شرحها في الموضوع الأول عن الفيروسات ..
أرجو قراءة الجزء الأول ليكون هذا الموضوع مترابطاً معه .

كلمة شكر

مثل هذا الموضوع يحتاج إلى أجهزة مصابة بالفيروسات لكتابته (مصائب قوم عند قوم فوائد) .. ولأني كنت بعيداً عن الأجهزة المصابة لم أتمكن من التعامل مع الفيروسات الجديدة .. لكن والحمد لله و بفضل الله تعالى ظهر هذا الموضوع للنور في فترة سفري السابقة .. حيث جلست (بعزبة) مجموعة من الأصدقاء و كانت لديهم أجهزة مصابة .. فمن باب شكر من أحسن إلي و تفضل علي بهذه المعلومات و سماحهم بتجاربي على أجهزتهم .. أتقدم بالشكر الجزيل لأصدقائي
أديب الكثيري و شكري باذيب و أخص عوض بهيان
لأنه كان خير المساعد و في بعض الأحيان أحسن مني ما شاء الله عليه و استفدت منه الكثير .. و للعلم كلهم يدرسون الهندسة الكيميائية ربنا يوفقهم و يغفر لهم و يتولاهم برحمته ..
و أيضاً أوجه شكر خاص للإخوة بمنتدى المشاغب ..
لأنه كثير من هذه المعلومات مأخوذة منهم .. ربنا يوفقهم و يبارك فيهم و يحفظهم و يجزيهم الفردوس الأعلى من الجنة و يجيرهم من النار و والديهم و أهليهم و محبيهم .. و للمسلمين جميعاً يا رب العالمين ..

هدف الموضوع

أكثر ما أسعى له في هذا الموضوع هو فهم طريقة عمل الفيروسات .. و كيفية إصابة أجهزتنا بها و أخيراً كيف نعرف أن أجهزتنا مصابة ..
كل هذا لأن الوقاية خير من العلاج ..
فالاعتماد على برامج مكافحة الفيروسات غير كافٍ و سيظهر ذلك في الشرح ..
و حماية الجهاز من الفيروسات أسهل بكثير من التخلص منها و من آثارها التخريبية ..



فيروسات
الموضوع



هنا أشرح تجاربي الشخصية مع فيروسات جديدة ومثيرة ..

فيروس W32/Sality.Y

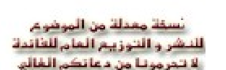
هذا الاسم الذي أعطاه الأفيرا لهذا الفيروس ..

و للأسف الفيروس يغير اسمه باستمرار .. و شركات الفيروسات تعطي أسماء مختلفة للفيروسات وسيظهر ذلك مع الفيروسات الأخرى ..

هذا الفيروس ينتشر في الجهاز و يندمج مع البرامج و اكتشافه صعب جداً .. لأنه لا ينسخ نفسه على سطح الأقراص الصلبة .. تعرف الإصابة بتعطل برنامج الحماية و عدم القدرة على إظهار الملفات المخفية .. ينسخ نفسه مباشرة على الفلاش ميموري (Flash Memory) إذا أوصلته بالجهاز المصاب و بأشكال متعددة تشترك في الحجم فقط .. قمت بإدخال و إخراج الفلاش عدة مرات بالجهاز لنسخ عدة أشكال للفيروس كما بالصورة ..



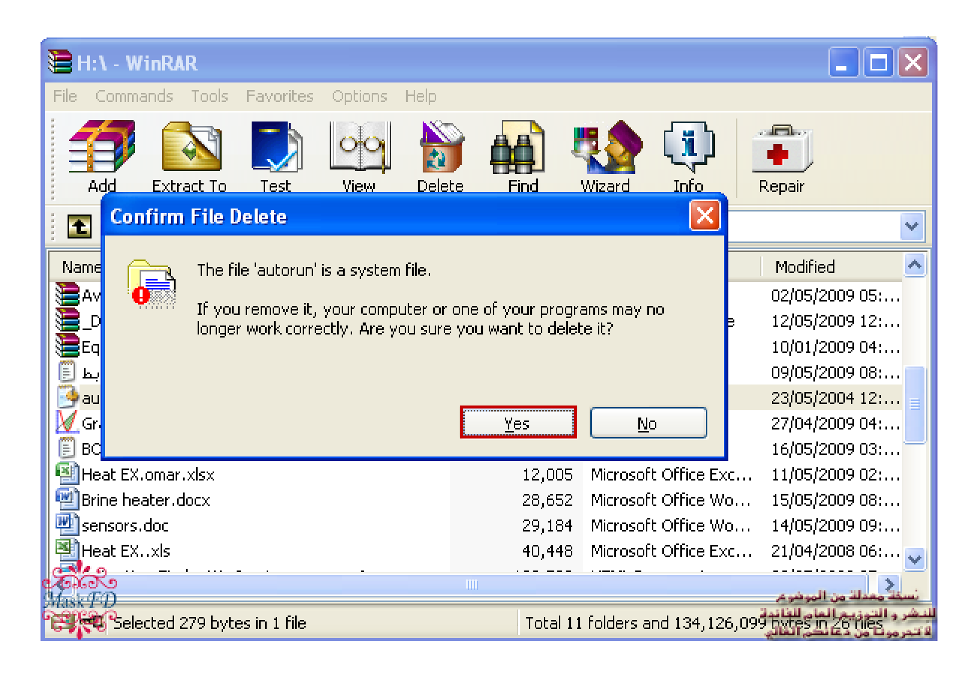


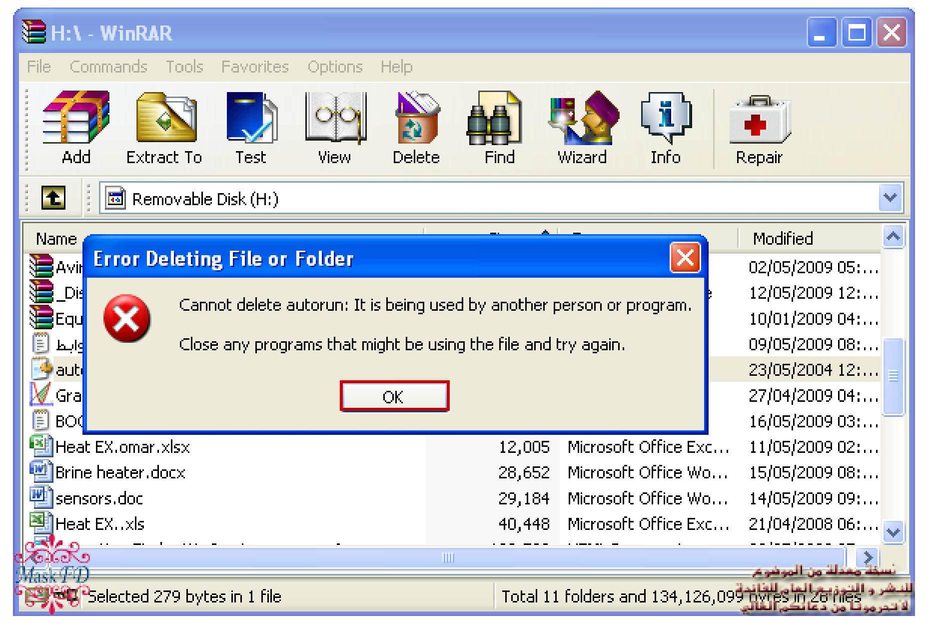




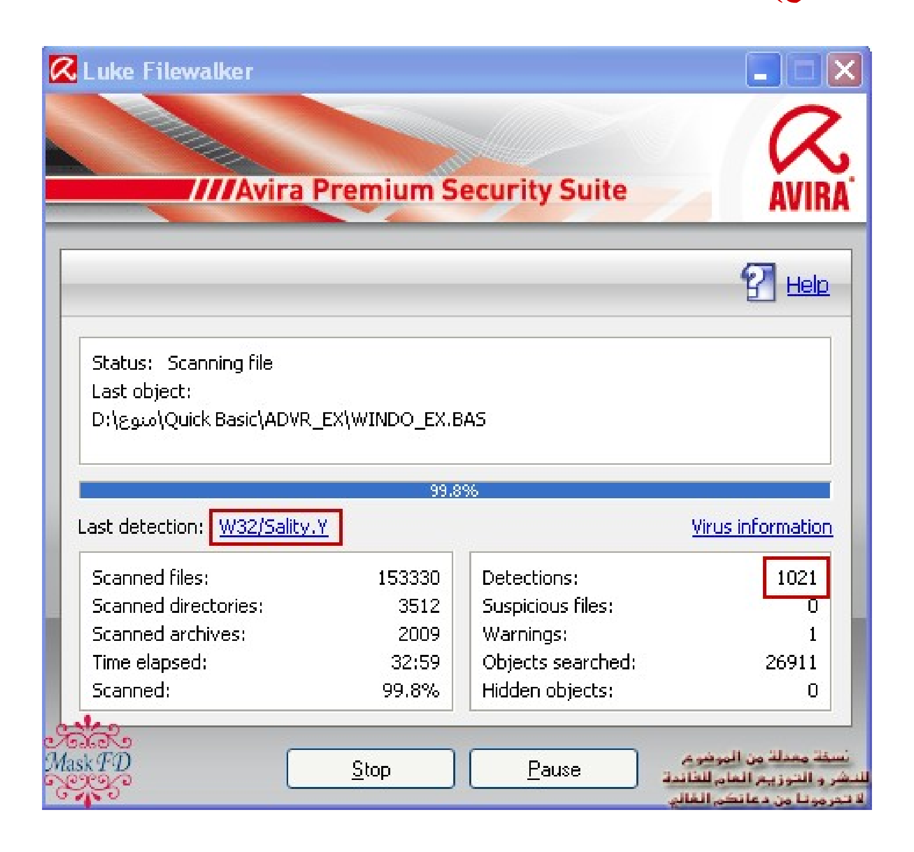
نلاحظ اختلاف الأيقونة و النوع و الاسم .. لكن الحجم نفسه .. و أيقونة اختصار MS-DOS هي في الحقيقة نفس الفيروس بامتداد PIF و عند البعض قد يظهر هذا الفيروس بهذا الامتداد لكن بدون أيقونة ..

عندما ينسخ نفسه على الفلاش لا يمكن حذف ملف autorun.inf بالطريقة العادية .. لكن يمكن حذف الفيروس ..





تمكنت بصعوبة من تحميل برنامج الأفيرا لأنه كانت فيه نسخة سابقة محملة منه .. لذلك من الأفضل حذف برامج الحماية ببرنامج متخصص لحذف البرامج و ليس عن طريق (إضافة و إزلة البرامج) .. و بعد الفحص اكتشف قرابة ألف ملف مصاب بالفيروس ..



و في جهاز آخر نقلت منه فيروس يسميه الأفيرا بنفس الاسم **W32/Sality.Y** رغم اختلاف الحجم و العمل .. حيث كان هذا الفيروس يأخذ اسم المجلد ثم يخفي المجلد الحقيقي .. و نقوم بالخطأ بفتح الفيروس اعتقاداً منا بأنه المجلد و تظهر رسالة خطأ .. امتداد هذا الفيروس **SCR** وهو نفس امتداد شاشات التوقف .. و لم يكن له ضرر يذكر ..









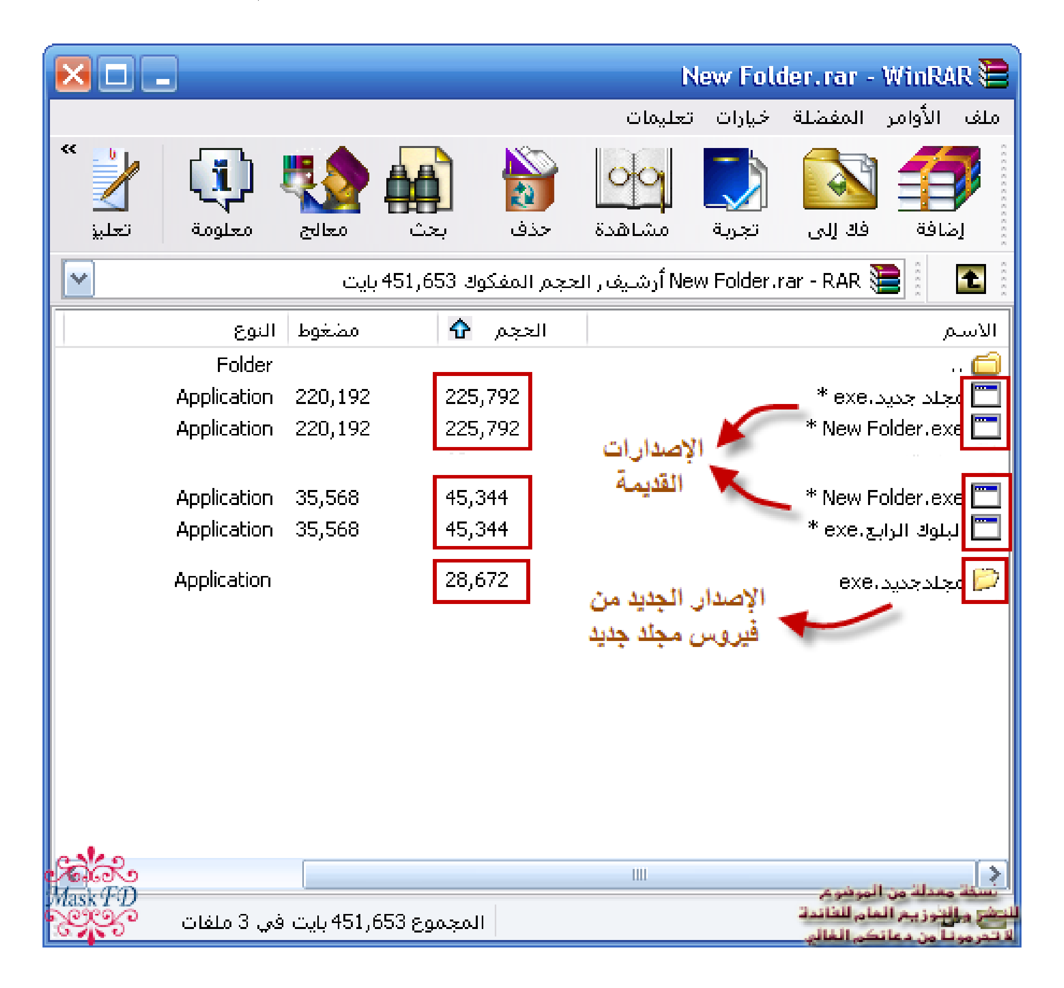
فيروس مجلد جديد New Folder بإصدار جديد

هذا الفيروس معروف للكثيرين و تم شرحه في الجزء الأول .. لكني وجدته في جهاز ابن عمي و لم يكتشف وقتها قبل خمسة أسابيع .. الآن اكتشفوه و حبيت تقارنوا فرق الحجم بينه و بين القديم .. و لاحظوا إن أيقونة الفيروس مشوشة قليلاً ..



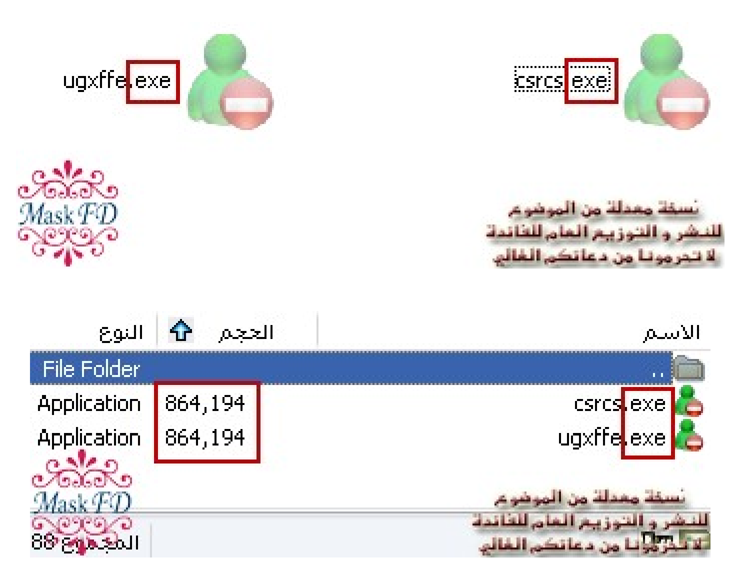


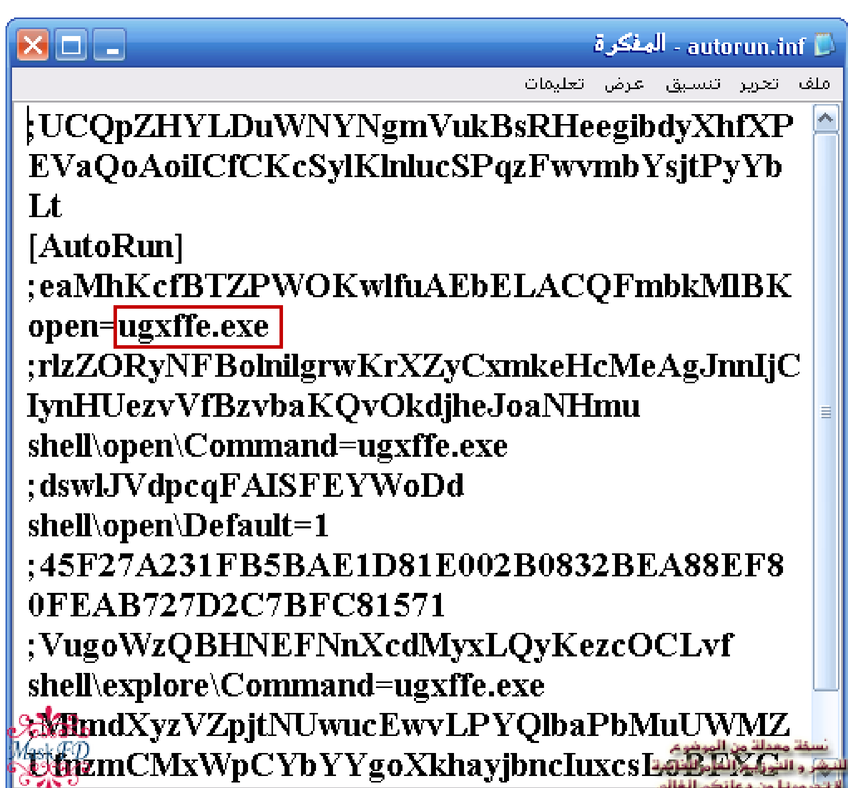
الصورة التالية مركبة لأنه لا يمكن جمع الفيروسات الثلاثة بنفس الاسم في مجلد واحد .. و بتلاحظوا إن الوينرار بيظهر الفيروس بعلامة التطبيق كما بالصورة ما عدا الفيروس الجديد يظهره كمجلد ويبدو أن الفيروس الجديد أكثر قوة لكن للأسف لم أرَ قدراته بعد ..



فيروس بعلامة الماسنجر

هذا الفيروس اكتشفه صديقي عوض بالفلاش ميموري وتوجد منه نسختين بنفس الحجم و الشكل وباختلاف الاسم (csrcs.exe) و (ugxffe.exe)
و للأسف الأفيرا إلى يوم كتابة الموضوع لا يكتشف هذا الفيروس .. مع ملاحظة أنه يوجد ملف نظام اسمه csrss.exe يشابه اسم الفيروس وسيظهر في الصور اللاحقة ..






```
;UCQpZHYLDuWNYNgmVukBsRHeegibdyXhfXP
EVaQoAoilCfCKcSylKlnlucSPqzFwvmbYsjtPyYb
Lt
[AutoRun]
;eaMhKcfBTZPWOKwlfuAEbELACQFmbkMlBK
open=ugxffe.exe
;rlzZORyNFBolnilgrwKrXZyCxmkeHcMeAgJnnIjC
IynHUezvVfBzvbaKQvOkdjheJoaNHmu
shell\open\Command=ugxffe.exe
;dswlJVdpcqFAISFEYWoDd
shell\open\Default=1
;45F27A231FB5BAE1D81E002B0832BEA88EF8
0FEAB727D2C7BFC81571
;VugoWzQBHNEFNnXcdMyxLQyKezcOCLvf
shell\explore\Command=ugxffe.exe
;MlmdXyzVZpjtNUwucEwvLPYQlbaPbMuUWMZ
UfnzmCMxWpCYbYYgoXkhayjbncIuxcsL...
```

وبما إني شكيت في هذا الفيروس .. رفعته إلى موقع **virustotal** لكن للأسف واجهة مشكلة مع الموقع .. فأعدت رفعه لموقع **novirusthanks** و اكتشف الفيروس **13** مضاد للفيروسات ..
و تلاحظوا من الصور إن كل شركة بتعطي اسم للفيروس ..
ما تدري تآخذ أي اسم منها ..



home blog p

NoVirusThanks
Free Virus & Malware Scan

Navigation Menu
- Scan a File
- Sample report
- Help
- About this Service

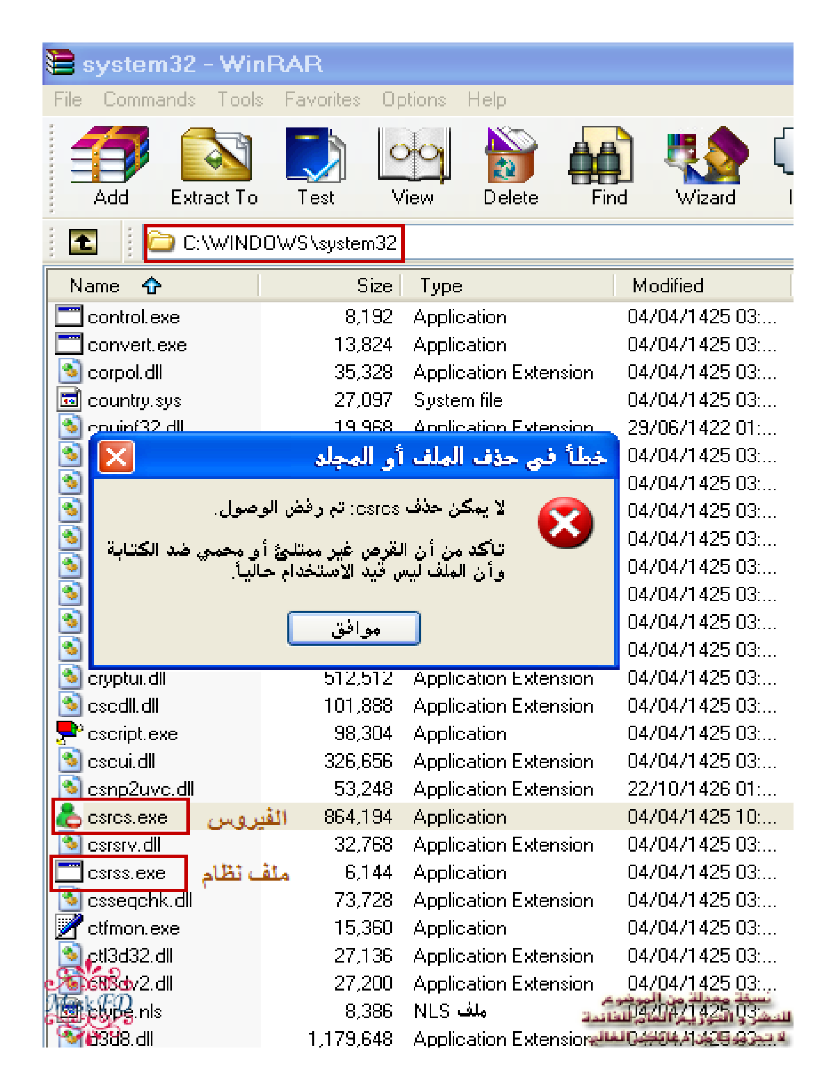
STATUS: Finished

File Information	
Report Generated:	3.7.2009 at 21.19.45 (GMT 1)
Time for scan:	52 seconds
File Name:	ugxffe.exe
File Size:	843 KB
MD5 Hash:	5ea2d147166d37b9f1104b9d0ae2008f
SHA1 Hash:	5A0D559A94A26A6E2F9BC0344AD3450BFFE690AB
Detection Rate:	13 on 24 (54.16%)

Antivirus	Sig version	Engine Version	Result
a-squared	03/07/2009	4.0.0.32	Worm.Win32.AutoIt!IK
Avira AntiVir	7.1.4.175	8.1.2.12	-
Avast	090702-0	4.8.1229	Win32:Trojan-gen {Other}
AVG	270.13.2/2215	8.0.0.0	-
BitDefender	03/07/2009	7.0.0.2555	Gen:Trojan.Heur.AutoIT.4304FBEBEB
ClamAV	03/07/2009	0.95.1	Trojan.Autoit-72
Comodo	1538	3.9	Unclassified Malware
Dr.Web	03/07/2009	5.0	-
Ewido	03/07/2009	4.0.0.2	-
F-PROT6	20090702	4.4.4.56	-
G-Data	19.6084	2.0.7309.847	Packed.Win32.Klone.bj A
Ikarus T3	03/07/2009	1001044	Worm.Win32.AutoIt
Kaspersky	03/07/2009	8.0.0.357	Packed.Win32.Klone.bj
McAfee	02/07/2009	5.1.0.0	-
Malware Hash Registry	03/07/2009	N/A	-
NOD32 v3	4213	3.0.677	Win32/Packed.Autoit.Gen
Norman	2009/07/03	5.92.08	Trojan Smalltroj.NUPW
Panda	21/05/2009	9.5.1.00	-
QuickHeal	03 July, 2009	10.0	-
Solo Antivirus	03/07/2009	8.0	-
Sophos	03/07/2009	4.32.0	Mal/Inet-Fam

لا يعني هذا بأن الأفيرا رديء .. لكن عشان تعرفوا إنه لا يمكن الاعتماد 100% على أي مضاد للفيروسات أو حتى 95% ..

و لم أتمكن من حذف الفيروس مباشرةً لأنه نسخ نفسه في مجلد النظام System32 وأكيد توجد نسخة منه تعمل في خلفية النظام للأسف لم أشاهدها بنفسي ..



أما آثار الفيروس .. فكانت سطحية بعد استخدام صديقي برنامج Combo Fix لكن ظهرت نافذة مزعجة مع بدأ تشغيل الويندوز ..



اضطررت لحذف جميع القيم التي باسم الفيروس في ملف **تسجيل الويندوز Windows Registry** بناءاً على اقتراح صديقي عوض ..

لا أنصح باستخدام هذه الطريقة لأنها غير مضمونة ..

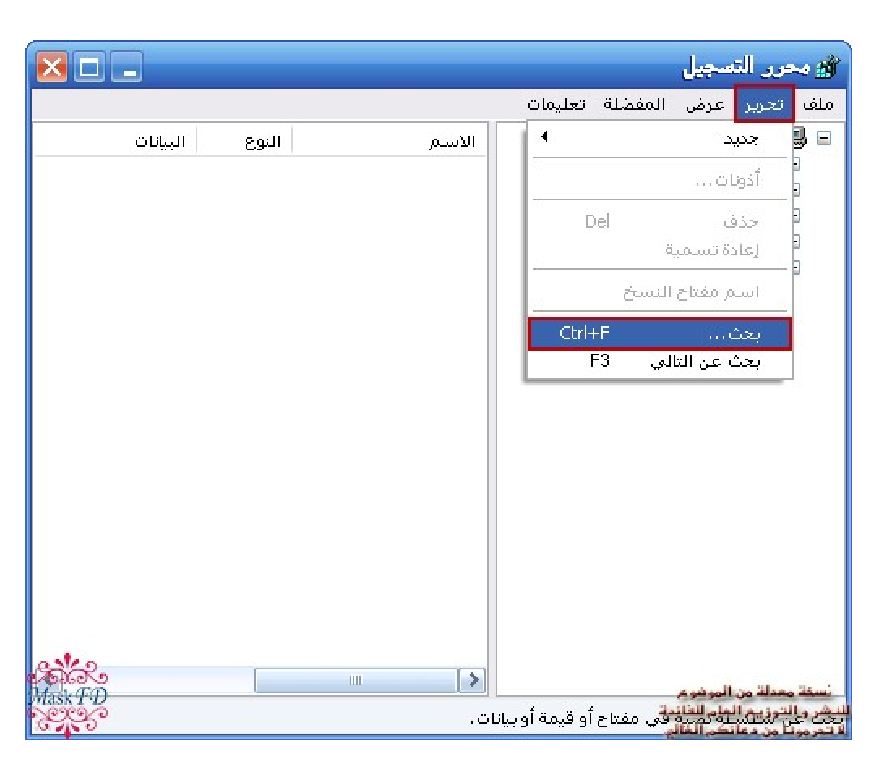
ولكن لمن يريد أن يعرف إليكم الطريقة :

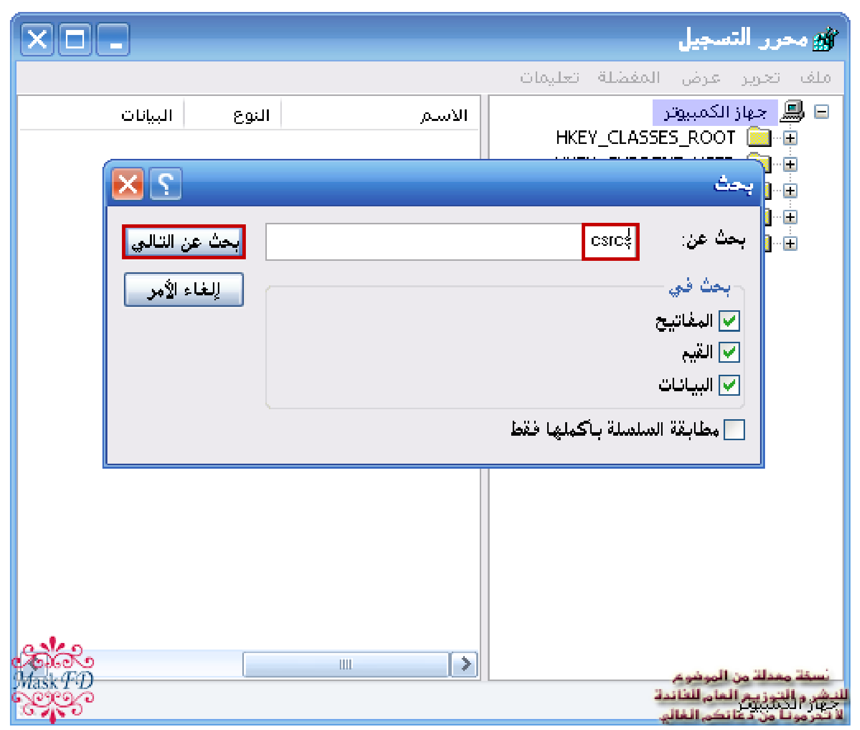
ندخل على ملف **تسجيل الويندوز (RegistryWindows)** من قائمة **ابدأ (Start)** ثم **تشغيل (Run)** ثم نكتب الأمر **regedit** ثم **موافق (OK)** .

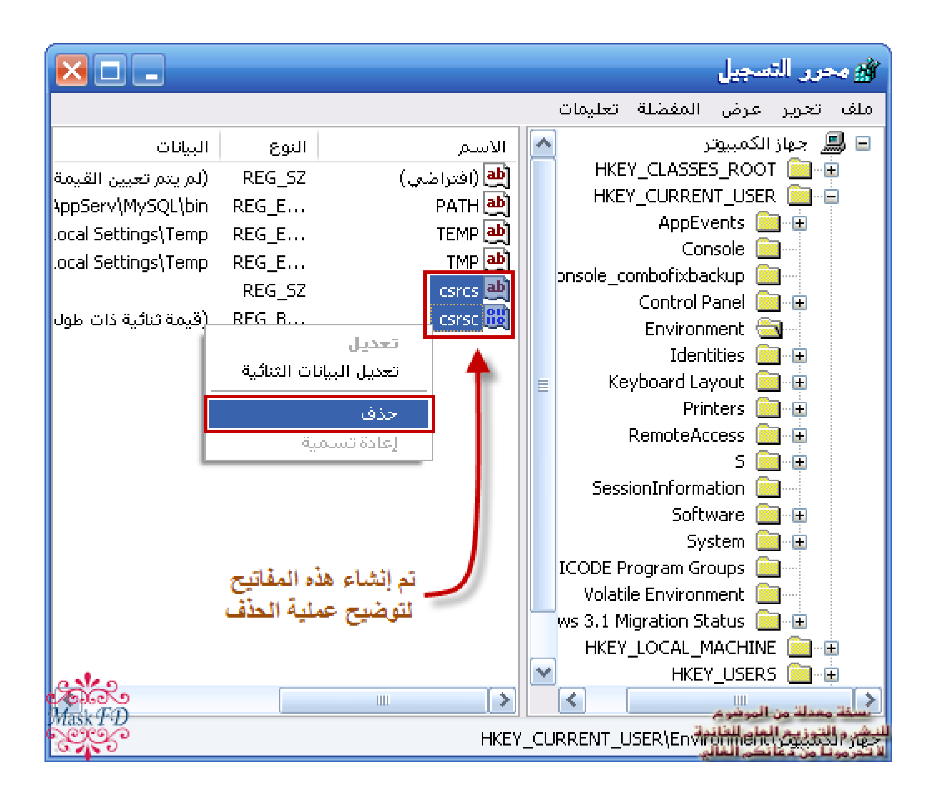


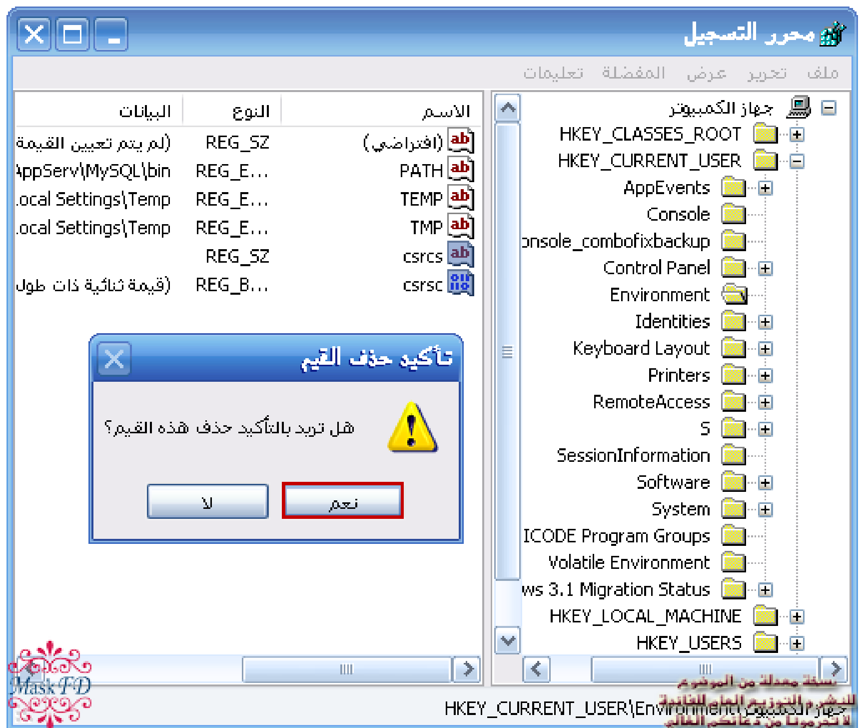


نتأكد من أن التحديد على جهاز الكمبيوتر .. إذا لم يكن ننقر عليه نقرة واحدة .. لأن البحث يبدأ من مكان التحديد .. ثم من القائمة تحرير Edit نختار الأمر بحث.. Search.. و نكتب اسم الملف الظاهر في رسالة الخطأ csrcs ثم نختار بحث عن التالي Search for Next و نقوم بحذف جميع القيم التي يظهر فيها إلى أن ينتهي من البحث في جميع ملف التسجيل الريجيستري ..









هذه الطريقة نجحت معاي .. لكني أنصح باستخدام برامج بدلاً عنها ..
و للأسف ما عندي خبرة في هذه الناحية ..

فيروس uxkl0apt

ما كان مفعل هذا الفيروس لكن لأن محتوى ملف الأوتورن autorun.inf غريب حبيت أرفعه لكم و الغريب لا يوجد اسم الفيروس بداخل الملف .. هذه صورة الفيروس ..

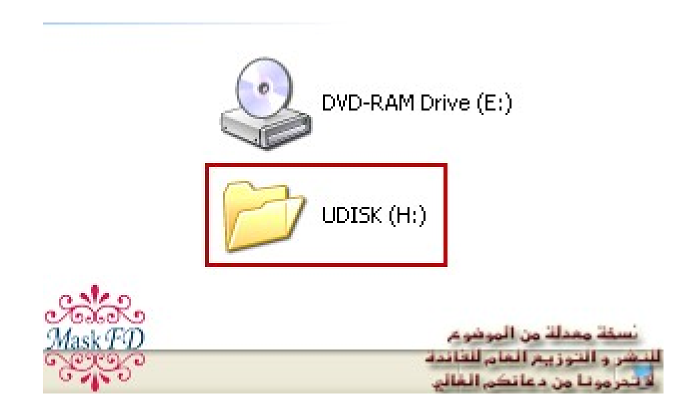




autorun.inf - المفكرة

ملف تحرير تنسيق عرض تعليمات

أيضاً تتغير أيقونة الفلاش ميموري Flash Memory إلى شكل مجلد كما بالصورة ..





كيف تــعرف أن جهازك مصــاب بالفيروســـــات؟

هذه بعض الطرق الشائعة لمعرفة الإصابة ..
إذا رأيت أحدها متحقق على جهازك قم بفحصه فوراً من الفيروسات ..

1- عدم القدرة على فتح إدارة المهام **Task Manager**
2- اختفاء أمر تشغيل **Run**
3- عدم القدرة على إظهار الملفات المخفية من خيارات المجلد **Folder Options**
يعني تفعل إظهار الملفات المخفية وتعمل موافق و ترجع الملفات بالاختفاء
4- التعطل المفاجئ لبرنامج الفيروسات أياً كان وعدم القدرة على تحميل أي مضاد آخر للفيروسات
5- بعض الأحيان يكون فيه بطئ ملحوظ في الجهاز
6- الفيروس غالباً ينسخ نفسه على سطح الأقراص لكن بما أن الفيروسات مخفية لن نتمكن من رؤيتها لذلك نستعرض الأقراص بالوينرار لأنه يظهر الملفات المخفية و ملفات النظام و لا يتأثر غالباً بعوارض الفيروس ..

كمثال عند فتح برنامج الوينرار ثم الدخول إلى القرص **C**
لو كان عندك فيروس ممكن تشوفه بهذه الهيئة :



تستطيع حذفه من هنا بمجرد تحديده و اختيار الأمر حذف الملفات **Delete Files**
أو اضغط على **Del** من لوحة المفاتيح **Keyboard**
هذا إذا كان من النوع البسيط ..



كيف تتصرف إذا أصابت الفيروسات جهازك؟

بعض الفيروسات يمكنك القضاء عليها بمجرد تحديث مكافح الفيروسات وعمل فحص شامل للجهاز وهذا الحل يناسب النوع الخفيف

يفضل أن يتم الفحص من الوضع الآمن .. أو عندما تدخل على القرص الصلب ببرنامج وينرار WinRAR يمكنك حذف الفيروس مثل المثال الوارد بالأعلى ..

طريقة الدخول للوضع الآمن Safe Mode

ندخل للوضع الآمن بعد إعادة تشغيل الجهاز والضغط على F8

ثم نختار الأمر Safe Mode

لتفصيل أكثر يمكنك زيارة هذا الرابط لموقع الأخ الكريم موفق غفر الله له ولوالديه و أهله وضع الرابط الأخ العزيز bosaad

طريقة الدخول إلى الوضع الآمن Safe Mode

و أيضاً ينصح بإيقاف استعادة النظام System Restore

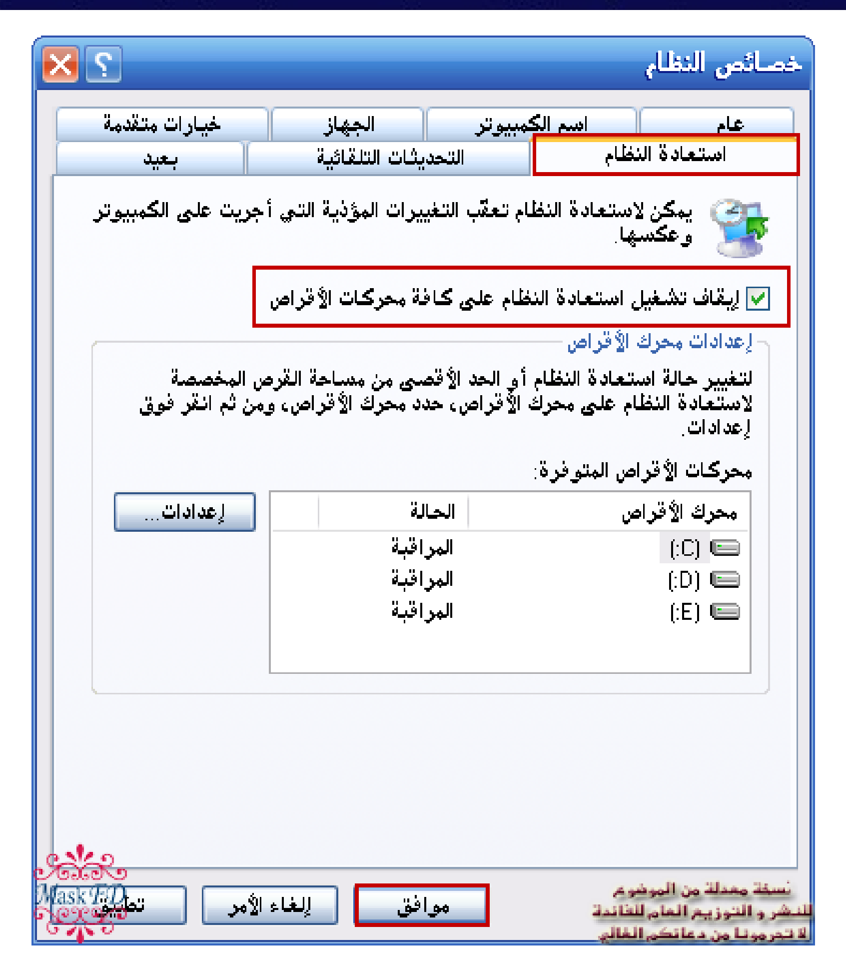
طريقة إيقاف استعادة النظام System Restore

ننقر بالزر الأيمن للفأرة على جهاز الكمبيوتر My Computer و نختار خصائص Properties ثم نختار التبويب استعادة النظام System Restore

ثم نضع علامة (صح) على إيقاف تشغيل استعادة النظام على كافة الأقراص Turn off System Restore on all Hard Drives

ثم نختار موافق OK .





إضافة قيمة من الأخ العزيز bosaad

الفائدة من إيقاف خاصية استعادة النظام هو أن هذه الخاصية تقوم بعمل نسخة للنظام وضمناً النسخة الفيروس الموجود على النظام. ومن هذه النسخة يعيد الفيروس انتشاره في الجهاز بعد حذفه لذلك يجب إيقاف خاصية استعادة النظام وإعادة تشغيل الجهاز وهذا يؤدي إلى مسح كل نسخ نقاط الاستعادة والتي تحتوي على نسخه "احتياطية" من الفيروس.

وبعد ذلك تعمل فحص للجهاز وتقوم بحذف الفيروس وتعيد تشغيل الجهاز وتعمل فحص آخر من جديد حتى يطمئن قلبك إلى أن الفيروس قد انتهى من جهازك وبعدها تفعل خاصية استعادة النظام وتقوم بعمل نقطة استعادة وقلبك مطمئن إلى أنها نظيفة وخالية من الفيروس.

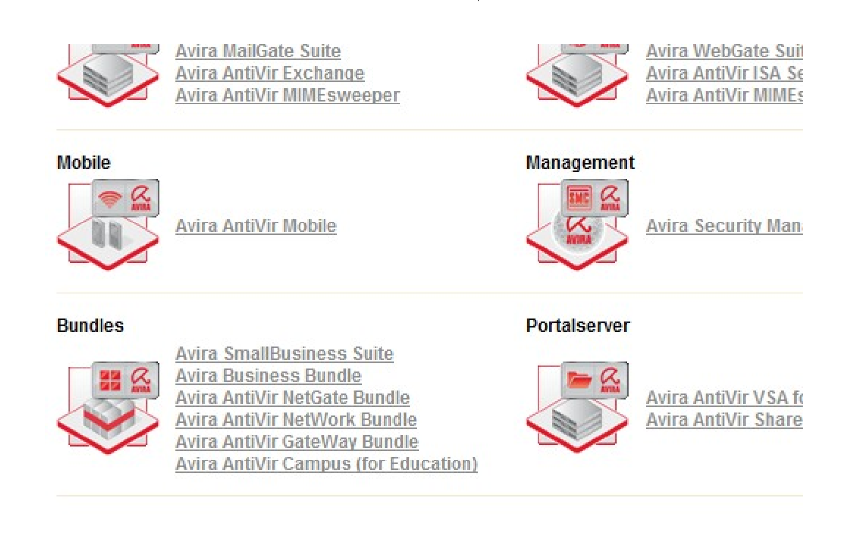
أما النوع الثقيل مثل الدودة Worm فغالباً لن تتمكن من استخدام مكافح الفيروسات لأنها ستقوم بتعطيله وستصبح مقيداً عند استخدام الويندوز لذلك يوجد حلان لهذا الأمر :

الأول

أن تقوم بتحميل Avira Rescue CD أو لو أمكنك أي مضاد فيروسات يفحص من خلال السيدي في وضع الدوس DOS وبآخر تحديث .. لكني أنصح بالأفيرا لأنه أفضل برنامج قابلته حتى الآن .. ولو كان ما اكتشف الفيروس المشروح بالأعلى لأنه لا يوجد برنامج حماية يحميك من كل الفيروسات .

السؤال هنا لماذا أفحص من خارج الويندوز؟

لأن الفيروسات تعمل في بيئة الويندوز لذلك يصعب حذفها ..لكنها لا تستطيع العمل في بيئة الدوس DOS و يصبح حذفها أسهل ..
يمكنك أن تحمل ملف بامتداد ISO من موقع الشركة و سأضع الرابط في قسم أدوات مساعدة ..
و الملف يتم تحديثه أكثر من مرة باليوم حسب كلام الشركة .. و بعدها تحرقه كصورة وليس كملف على سيدي ببرامج حرق السيديات مثل النيرو Nero
و بالطبع تغير في اعدادات البيوس BIOS في جهازك ليتم الإقلاع من السيدي أولاً ..
أترككم مع الصور من تحميل هذا الملف من موقع الافيرا Avira إلى فحص الجهاز ..
ندخل موقعهم www.avira.com



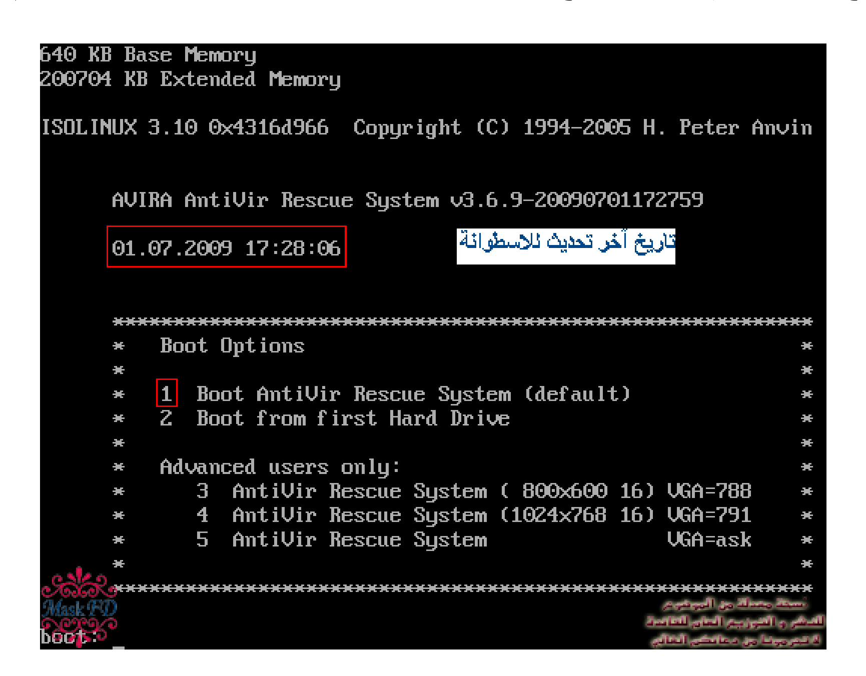
General downloads



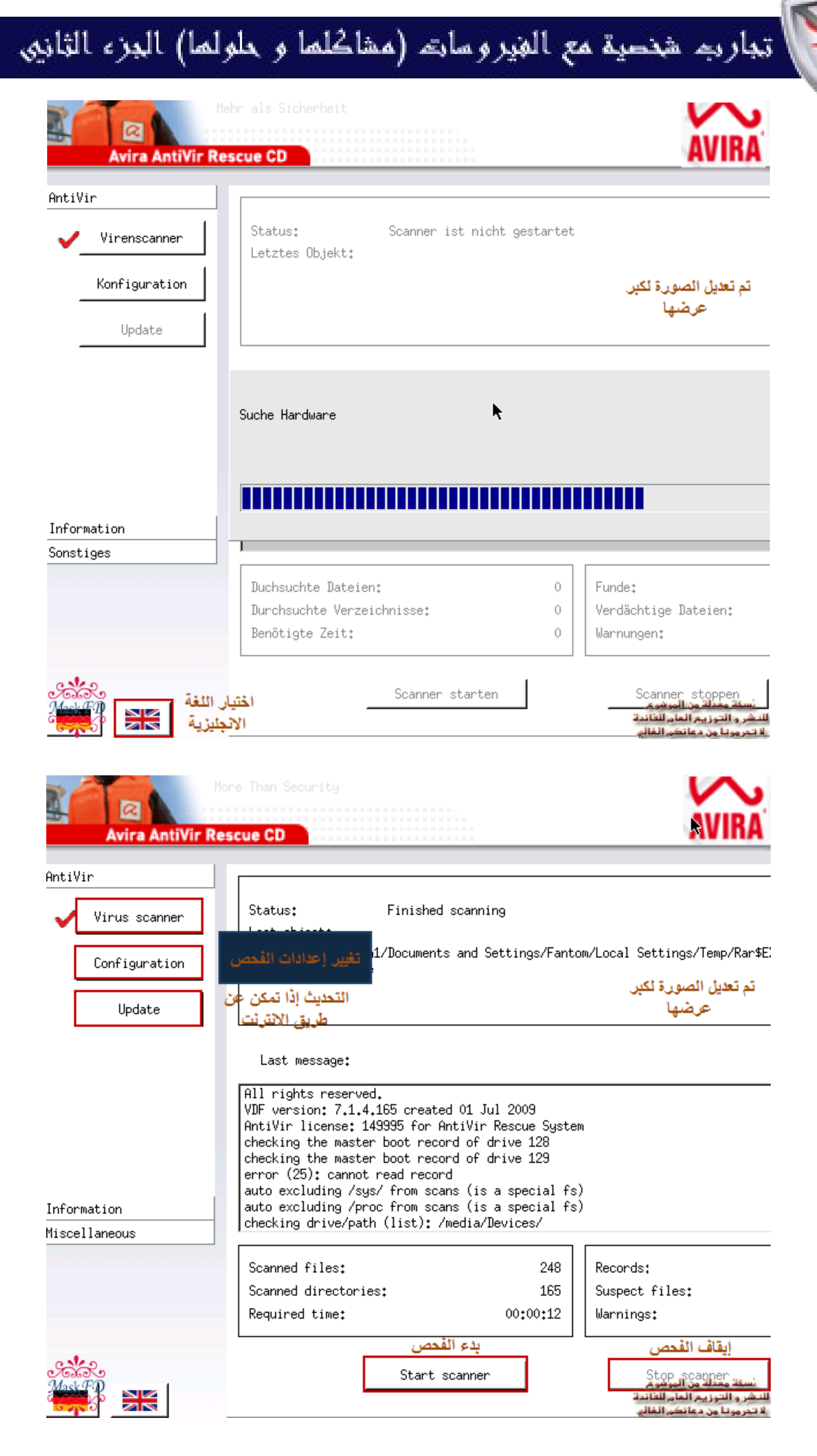




بعدها يبدأ التحميل و الذي أظنه يدعم الاستكمال ثم بعد حرقه على سيدي و الإقلاع منه تظهر هذه النافذة .. إذا تركته بدون اختيار أي رقم يقلع من السيدي تختار الرقم ثم Enter
1 للإقلاع من السيدي و 2 للإقلاع من القرص الصلب و بقية الخيارات متقدمة لم أجربها



يبدأ بتحميل ملفات وربما فحص جزئي للقرص ونختار اللغة من الأسفل كما بالصورة



أنصح بتغيير إعدادات الفحص باختيار حذف الملفات المصابة أو محاولة إصلاحها كما بالصورة
نختار الأمر **Configuration**



Avira AntiVir Rescue CD

AntiVir
Virus scanner
Configuration
Update
Information
Miscellaneous

Scan mode
Scan all files
Smart scan
Scan boot sectors only

Action at malware discovery
Protocol malware records only
Remove infected files — حذف الملفات المصابة
Try to repair infected files
Rename files, if they cannot be removed?

محاولة إصلاح الملفات المصابة و الخيار الثاني إعادة تسميتها إذا عجز عن الحذف

Extendet risk categories
Scan for dialers
Scan for joke programs (Jokes)
Scan for games
Scan for spyware (SPR)

Mask FD

More Than Security
Avira AntiVir Rescue CD
AVIRA

AntiVir
Information
Miscellaneous — ننقر هنا لتظهر هذه الخيارات
Commandline
Shutdown

تم تعديل الصورة لكبر عرضها

Turn off computer
Shutdown — إيقاف تشغيل الجهاز
Restart — إعادة التشغيل
Cancel — إلغاء الأمر

Lindauer Str. 21
88069 Tettnang
Germany

http://www.avira.com
Copyright 2008

Mask FD

الثاني

لا أعتبره حلاً لأنه أعجز الحلول .. وهو الفورمات أو تهيئة القرص الصلب Disk Format لكن إذا اضطررت إليه قم بعمل تهيئة سريعة للقرص Quick Format القرص المنصب أو الموجود عليه ويندوز و غالباً يكون C لأنها لا تضر الهارديسك Hard Disk بعكس الفورمات العادي Format حيث أن كثرة استخدامه تؤثر في عمر القرص الصلب ..

بعض الإخوة بيقولون إن الفيروس رجع بعد الفورمات ..
السبب غالباً يرجع لأمرين :

أحدهما
الدخول للأقراص الأخرى بعد الفورمات مباشرة و قبل تحميل مضاد الفيروسات ..
لأن الفيروس لا يزال موجوداً بالأقراص الأخرى ..
والآخر
استخدام برنامج الفيروسات القديم .. والذي سيكون غالباً مصاباً بالفيروس ..
فيرجع الفيروس مرة أخرى ..

لذلك لازم تحمل نسخة جديدة من برنامج الفيروسات .. أو تأخذ نسخة نظيفة من صاحبك مثلاً ثم تقوم بتنصيبها على الجهاز ..

ملاحظة :
قد لا يعمل نظام ويندوز لديك بعد الفحص لأن مكافح الفيروسات ممكن يحذف ملفات النظام المصابة بالفيروس ..
لذلك لازم تنسخ ملفاتك الهامة قبل هذه العملية ..



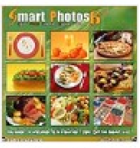
ملفات ليست بفيروسات

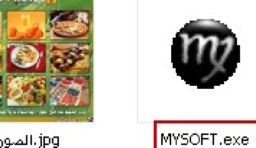
لأنها مخفية قد يعتقد البعض بأنها فيروسات .. لكنها معظمها ملفات غير تنفيذية أي من النوع اللي يشتغل بالنقر المزدوج عليه مثل exe,scr,com,bat.pif

Autorun.inf

هذا الملف يشغل الفيروس المرافق له .. لكنه ليس فيروساً .. و ممكن تجده في أي سيدي تعليمي أو حق برامج لأنه يشغل العرض التقديمي اللي في السيدي .. أيضاً عن طريقه تضع أيقونة للأقراص ..

لذلك برامج الفيروسات غالباً لا تحذفه و تستطيع حذفه بشكل يدوي كمثال لسيدي يحتوي صور لمأكولات منوعة لا تجوعوا بسببه ^_^


الصورة.jpg


MYSOFT.exe

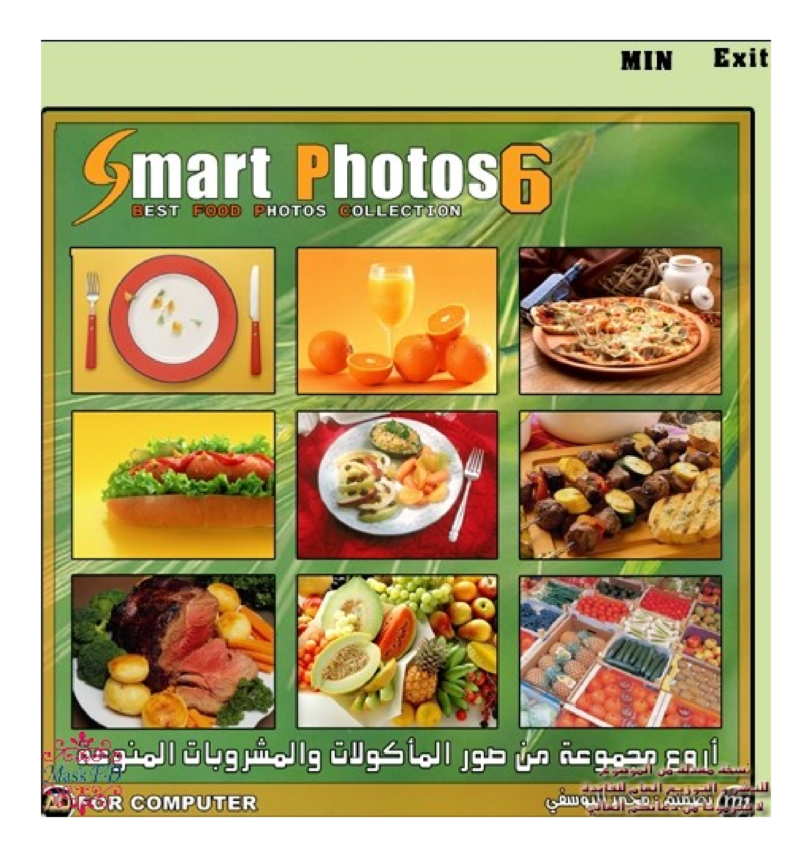

autorun.inf

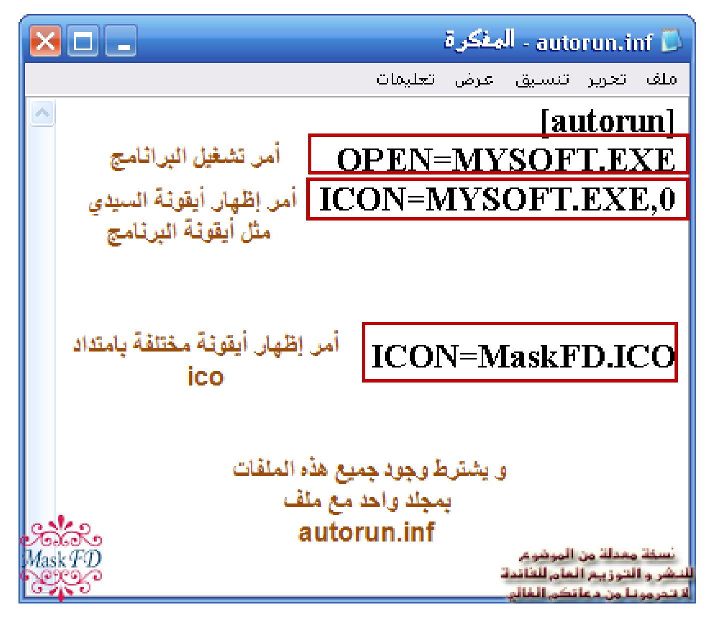

smart photos 6

هذا محتوى سيدي للصور

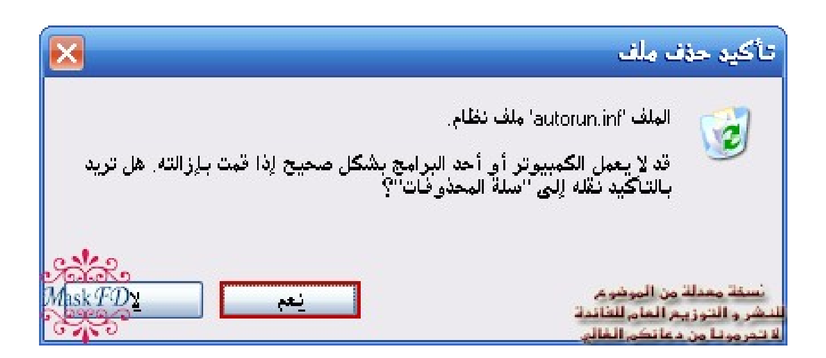


نسخة معدلة من الموضوع
للنشر و التوزيع العام للفائدة
لا تحرمونا من دعائكم الغالي





تظهر رسالة تحذير عند حذفه بأنه ملف نظام ..
لكن لا توجد مشكلة من حذفه .

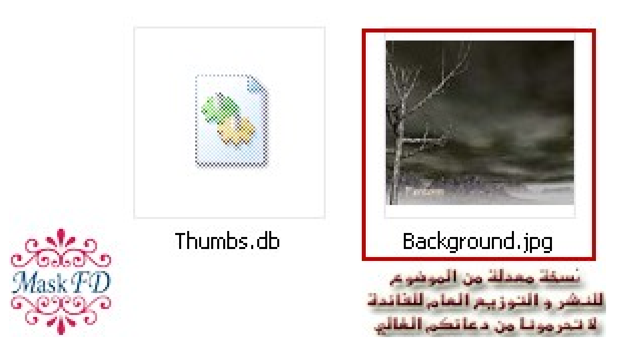


Folder Settings ومجلد desktop.ini

تجدهم في المجلدات التي تحتوي على خلفية .. desktop.ini أعتقد يكون فيه تحديد لون الخطوط في هذا المجلد وصفات أخرى و Folder Settings توضع به صورة الخلفية و تكون باسم Background.



و هذه صورة الخلفية من داخل مجلد **Folder Settings**



Thumbs.db

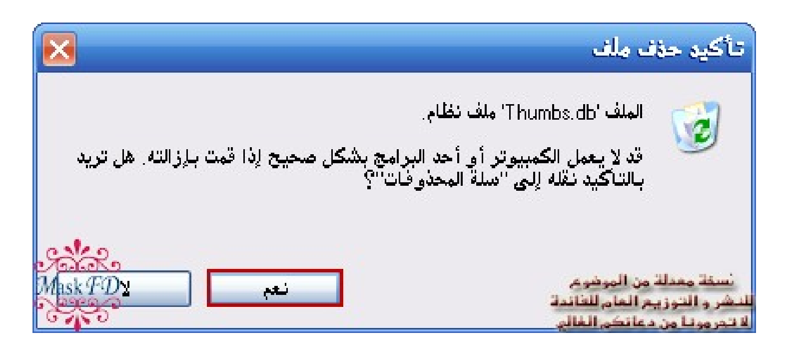
ملف يتكون في كل مجلد فيه صور أو فيديو تعمل فيه عرض **المصغرات** .. أعتقد لتسريع عرض المصغرات يمكنك حذفه بسهولة لكن بشرط تغيير عرض الملفات في المجلد إلى غير المصغرات لأنه وقتها يكون مستخدم .. وبعض الأحيان يقبل الحذف في وضع المصغرات ..

و عند حذفه تظهر رسالة بأنه **ملف نظام** .. توافق على الحذف ..

وللتأكد من عدم ضرر ذلك ارجع عرض الملفات إلى المصغرات وسيعود **Thumbs.db** مرة أخرى .. ويختلف حجم هذا الملف باختلاف عدد الملفات وأعتقد نوعها ..

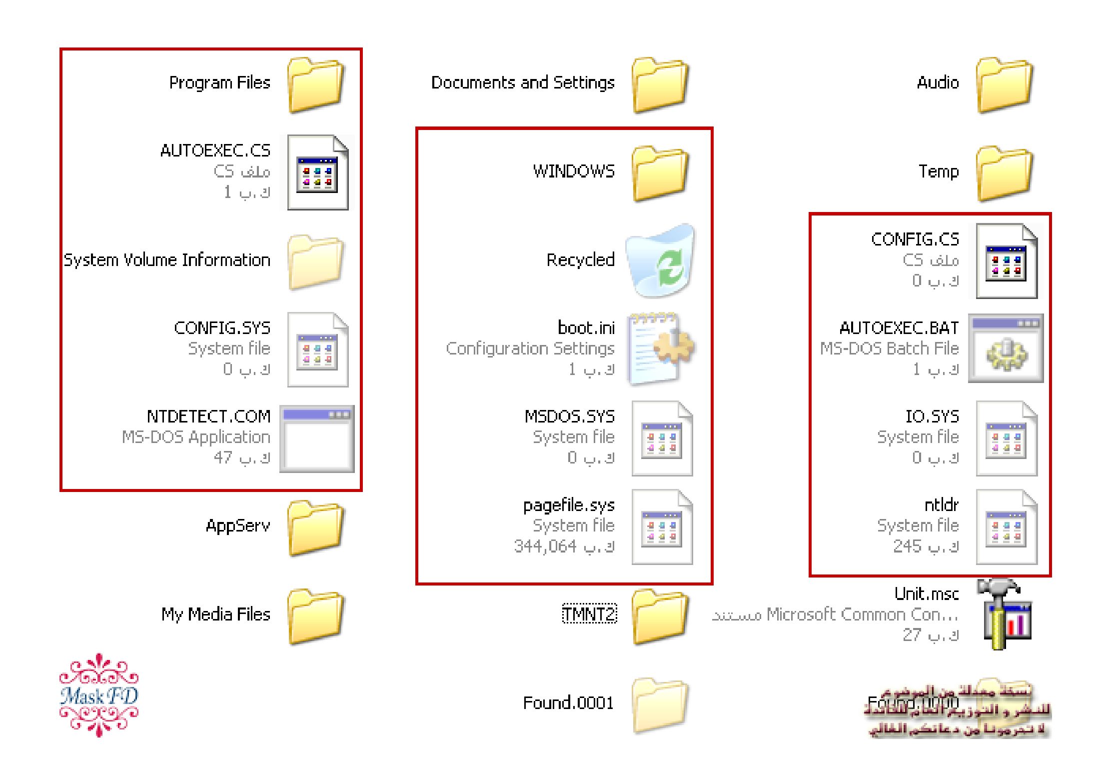






ملفات النظام الموجودة على سطح القرص الصلب

على القرص المحمل عليه ويندوز توجد ملفات كثيرة مخفية تابعة للنظام وتوجد بعضها على الأقراص الصلبة الأخرى .. **بالطبع لا يمكننا حذفها** .. منها **boot.ini** المسؤول عن ترتيب أنظمة التشغيل عند بداية تشغيل الجهاز و تحديد وقت الانتظار غالباً يكون 30 ثانية ..وغيرها من الملفات الموضحة بالصورة:



ملفات النظام الموجودة على سطح القرص الصلب الخارجي

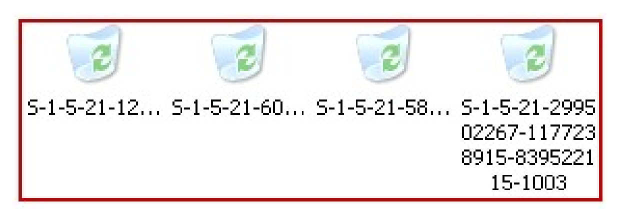
تجد هذه المجلدات مثل **RECYCLE.BIN$** و **RECYCLER** كما بالصورة:



وتحتوي على سلة المحذوفات ولكن بشكل متعدد .. بعضها يقبل الحذف بدون مشاكل والآخر لا .. وتختلف في المجلدين كما بالصور ..









بقايا فحص أخطاء القرص

بعد فحص أخطاء القرص الصلب تبقى مجلدات على سطح القرص بهذه التسمية Found.0000 يمكن حذفها بدون مشاكل ..





ملفات بامتداد TMP

غالباً تكون الملفات المؤقتة Temporary بهذا الامتداد و يمكن حذفها أيضاً ..







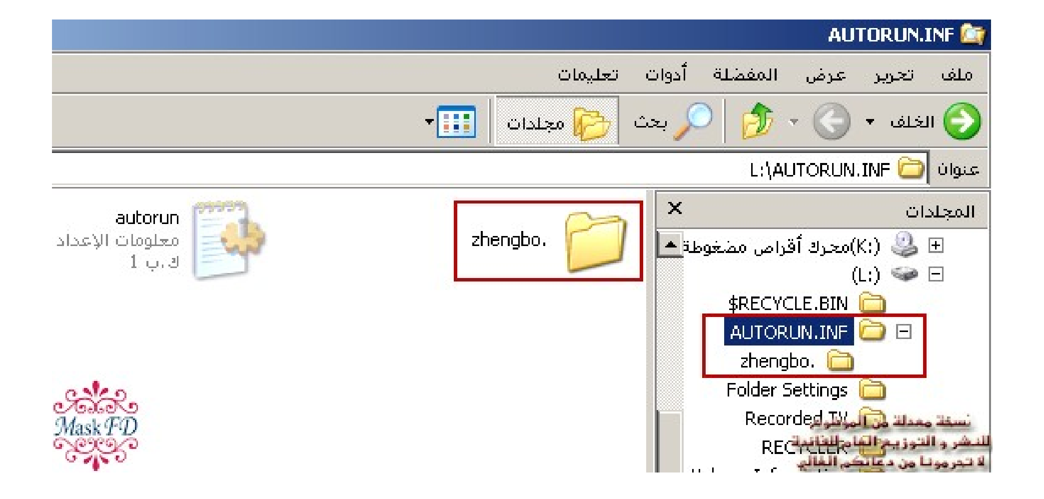


AUTORUN.INF داخل مجلد باسم .zhengbo

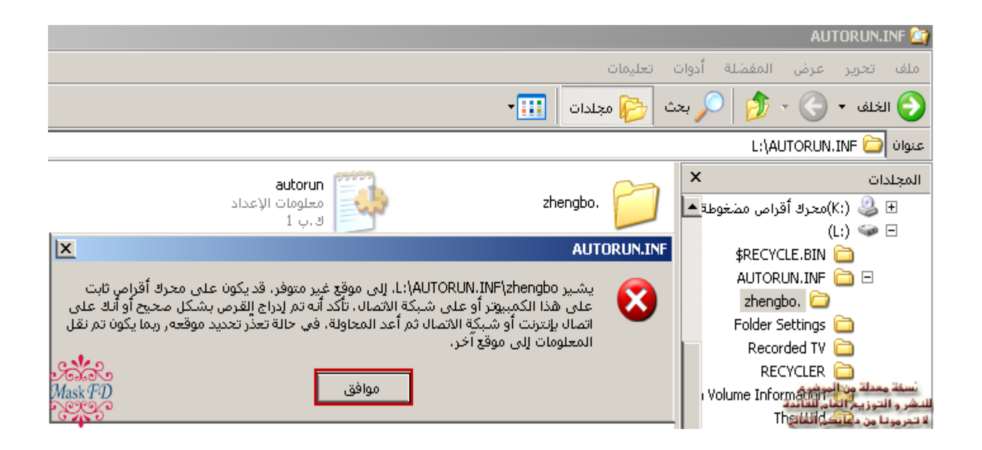
هذا المجلد مذكور في الموضوع الأول لكن في مشاركات الأعضاء لأني ما كنت قابلته وقتها ..
الآن عندي بعض الصور و كيف تحذف آثاره .. وللعلم يكون موقعه على سطح الأقراص الصلبة أو الفلاش ..
وهو ليس فيروس كما كنت أعتقد ويعتقد الكثيرون ..
ولكنه ينتج من برنامج متخصص للحماية من فيروسات التي تأتي من الفلاش ميموري حسب الرأي الراجح
للأخ المراقب سلطان العبدلي ..
ويبدو وظيفة الملف منع الفيروس من نسخ نفسه على الفلاش ميموري حيث لا يمكن استبداله و حذفه لكن لمن يريد حذفه يمكنه متابعة القراءة .
هذا هو المجلد وطبعاً مخفي ولازم نظهر الملفات المخفية وملفات النظام



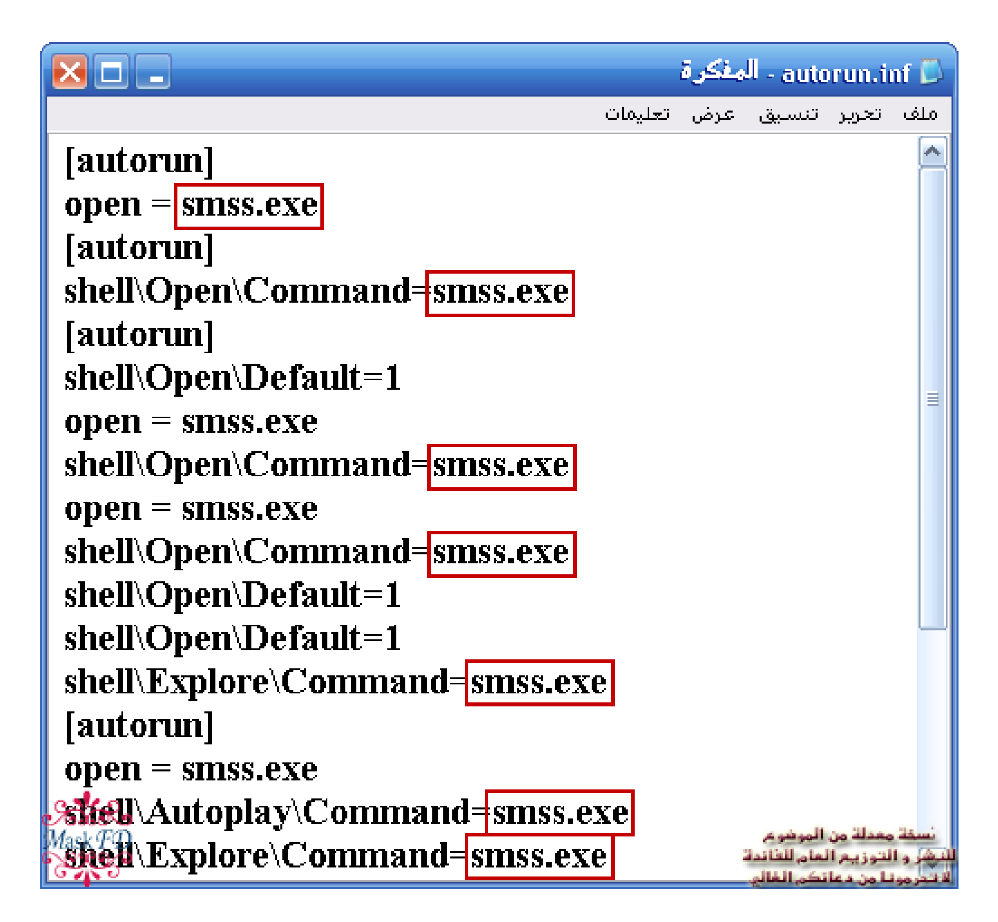
هذه الصورة بعد دخولي له من مستكشف الويندوز Windows Explorer



عندما حاولت الدخول إلى مجلد zhengbo. ظهرت رسالة الخطأ هذه .



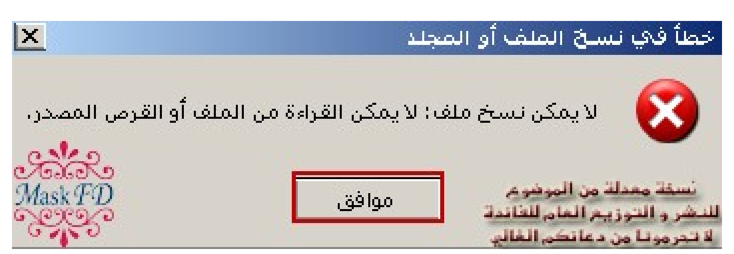
ملف الأوتورن autorun.inf يدل على إن اسم الفيروس اللي كان موجود هو smss.exe ويبدو البرنامج ينقل الفيروس لهذا المجلد لكي لا يتم تفعيله هذا محتوى ملف الأوتورن autorun.inf.



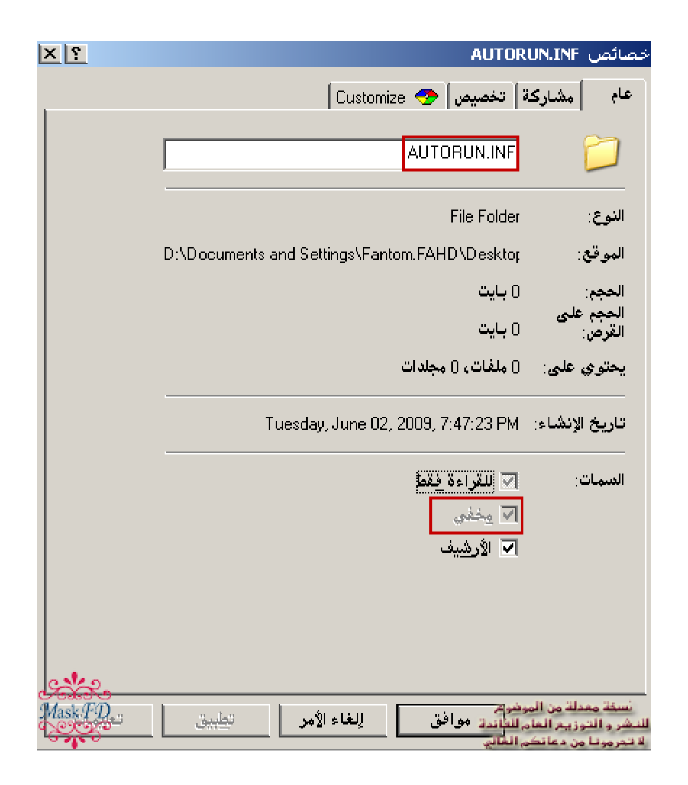

```
[autorun]
open = smss.exe
[autorun]
shell\Open\Command=smss.exe
[autorun]
shell\Open\Default=1
open = smss.exe
shell\Open\Command=smss.exe
open = smss.exe
shell\Open\Command=smss.exe
shell\Open\Default=1
shell\Open\Default=1
shell\Explore\Command=smss.exe
[autorun]
open = smss.exe
shell\Autoplay\Command=smss.exe
shell\Explore\Command=smss.exe
```

لا يمكن حذف الملف بالطريقة العادية .. أو حتى نقله لمكان آخر ..

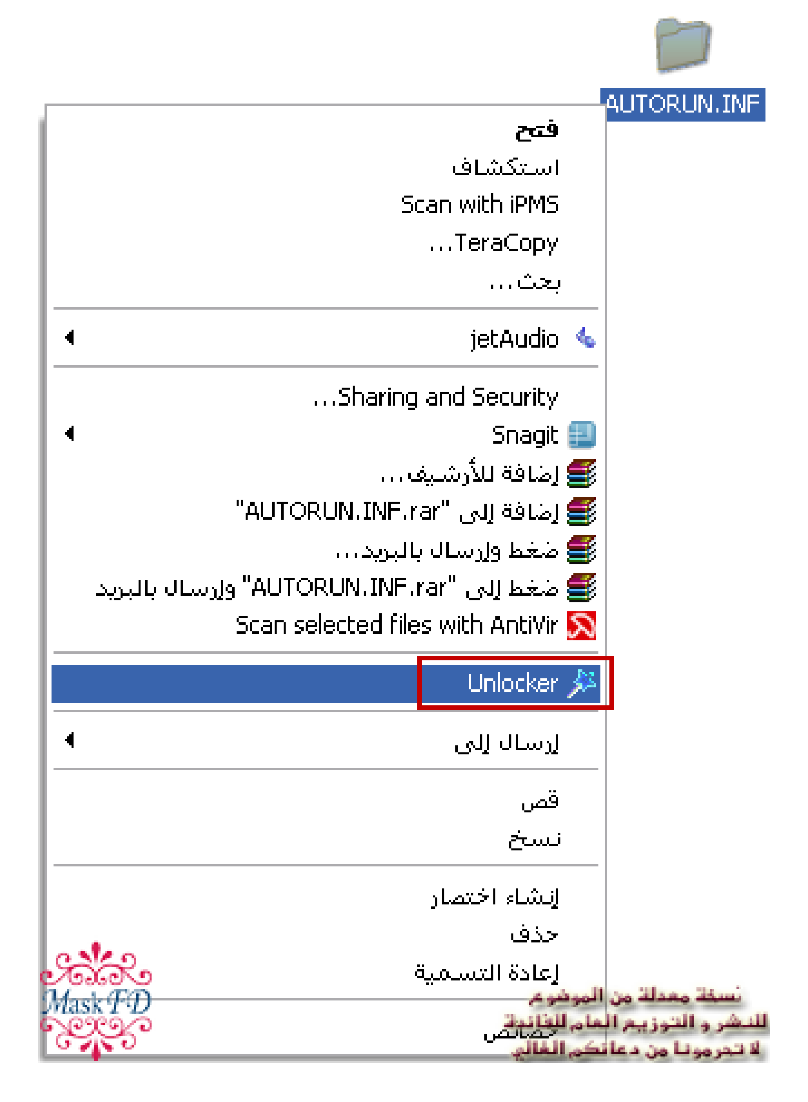


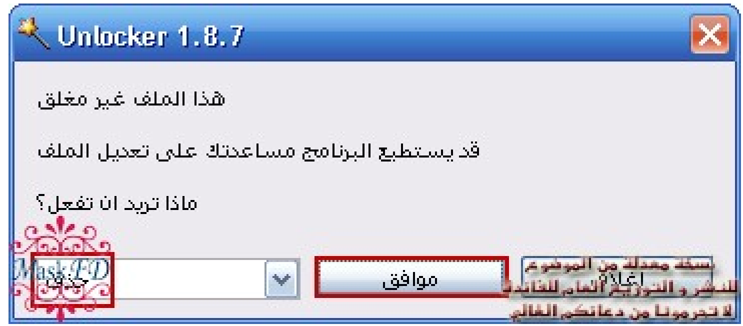


وطبعاً المجلد مخفي ولا يمكن إظهاره ..



هذا الأثر غير الضار لا يحذفه برنامج الفيروسات .. مثل ما يترك ملف الأوتورن autorun.inf و الذي يمكننا إزالته يدوياً .. قمت بتحميل برنامج Unlocker 1.8.7 .. يقوم هذا البرنامج بحذف هذا المجلد بدون مشاكل .. فقط ننقر على المجلد باليمين ونختار الأمر unlocker ثم نختار الأمر حذف Delete ثم موافق OK بعدها تظهر نافذة باكتمال العملية ثم موافق OK .







أدوات مساعدة

طبعاً بالأول لازم يكون عندك برنامج حماية ..
أنصح باستخدام أحد البرامج التالية:
الأفيرا Avira أو الكاسبر سكاي Kaspersky أو النود 32 Nod32 أو البت ديفيندر Bit-Defender أو الأفاست Avast أو AVG و غيرها كثير لكن هذا اللي أعرفه واستحق التجربة .. أهم شيء أشدد عليه تحديث البرنامج لأنه بدونه ما بتستفيد ..
مع ملاحظة إنه غير ممكن استخدام برنامجين منها في نفس النظام لأنه يسبب تضارب ومشاكل للنظام .. لكن ممكن تستخدم برامج أخرى للمالوير Malware أعتقد معناها مضادات البرامج الضارة معها بدون مشاكل ..
و هنا أحب أوضح بعض الفروق بين إصدارات مضادات الفيروسات ..

الإصدار المجاني
بعض الشركات بتصدر إصدار مجاني .. لكن محدود المزايا ..
يمكن تغطية هذه المحدودية ببرامج مساعدة ..

إصدار الحماية من الفيروسات Antivirus
يحميك من الفيروسات و بكامل الخصائص .. لكن ما يحميك من الاختراقات والهكرز ..
إذا ما عندك انترنت أو موصول بشبكة محلية يكفيك هذا النوع ..

الإصدار الشامل Security
يحميك من الفيروسات و الاختراقات .. لأن فيه جدار ناري FireWall وهو لأصحاب الشبكات و الانترنت ..

بعد هذه المقدمة ندخل على البرامج .. جميعها مفحوصة بالافيرا حتى الموجودة بالمواضيع لأني حملتها عندي .. لكن لزيادة الأمان لازم تفحصوها بأنفسكم ..

برنامج RRT
برنامج يرجع خيارات المجلد و إدارة المهام و أمور أخرى يلغيها الفيروس ..
وضعت الإصدار RRT 2.0 و آخر إصدار RRT 4.9
البرنامج مجاني للاستخدام المنزلي ..
البرنامج مرفوع على الميديا فاير Mediafire اضغط على صورة التحميل مشكوراً ..



برنامج Unlocker 1.8.7

لحذف وإعادة تسمية ونقل الملفات المستعصية ..

البرنامج مجاني للاستخدام المنزلي ..

البرنامج مرفوع على الميديا فاير Mediafire اضغط على صورة التحميل مشكوراً ..



يمكنك مشاهدة شرح مفصل للبرنامج على الرابط

[۩MaskFD۩برنامج Unlocker 1.8.7 لحذف وإعادة تسمية ونقل الملفات المستعصية+الشرح تفصيلاً]

اسطوانة الافيرا Avira Rescue CD

عبارة عن ملف بامتداد ISO بعد تحميله تقوم بحرقه على CD و تخلي إقلاع الجهاز من السيدي ليفحص الجهاز من الفيروسات .. البرنامج من موقع الشركة وأعتقد يدعم الاستكمال .

طبعاً الاسطوانة مجانية .

الحجم = 52 MB

DOWNLOAD

الافيرا فقط هو المجرب عندي .. لكني وجدت اسطوانات أخرى في موضوع الأخ المراقب madeee وحبيت أضيفها للفائدة وأعتقد كلها تدعم الاستكمال و كلها مجانية و حجمها يتغير ويتزايد مع التحديثات الجديدة .

اسطوانة الكاسبر سكاي KasperSky Rescue CD

الحجم = 114 MB



اسطوانة F سكيور F-Secure Rescue CD

الملف مضغوط بامتداد ZIP لكن الاسطوانة امتدادها ISO .

الحجم = 152 MB



اسطوانة البت ديفيندر BitDefender Rescue CD

رابط هذه الاسطوانة يتغير بتاريخ تحديثها .. لذلك بعد ما تدخل على هذا الرابط ننقر على الرابط الموضح بالصورة و يبدأ بعدها التحميل .

الحجم = MB 260



Index of /rescue_cd

Name	Last modified	Size
Parent Directory		-
BitDefenderRescueCD_v2.0.0_3_08_2009.iso	03-Aug-2009 11:55	260M
BitDefenderRescueCD_v2.0.0_3_08_2009.iso.md5	03-Aug-2009 11:54	75
Old/	02-Mar-2009 09:57	-

اسطوانة دكتور ويب min DrWeb Live CD

الحجم = MB 66



برامج في مواضيع للأخ الغالي ملك البرامـــج

اخر نسخ جديدة Avira) Avira AntiVir Premium,Avira AntiVir Personal,) Premium Security

ملف تحديث الافيرا Avira Antivir Virus Definition File Update June 29,)) ((2009

شرح اداة صغيرة لفحص اي ملف بـــــ 41 ـــــــ مضاد للفيروسات

اعمل نسخة احتياطية لاي شي في الجهاز مع تحديث تلقائي واسترجعها في ثواني (جديد مع الشرح

برامج في مواضيع للأخ العزيز المراقب سلطان العبدلي

ادوات للتخلص من اغلب مشاكل الجهاز(صادف الاكسبلورر مشكله-الاوتورن)وغيرها

برنامج لتنظيف الجهاز من التروجان والماليوار Malwarebytes Anti-Malware 1.38

14-3-2009 اداه SDFix v1.240 لازاله الفيروسات

برامج في مواضيع للأخ العزيز المخفي 2000

إصلاح أكثر مشاكل الريجيستري شيوعاً

اداه جديده لحذف اي برنامج حمايه في جهازك



مواقع مساعدة

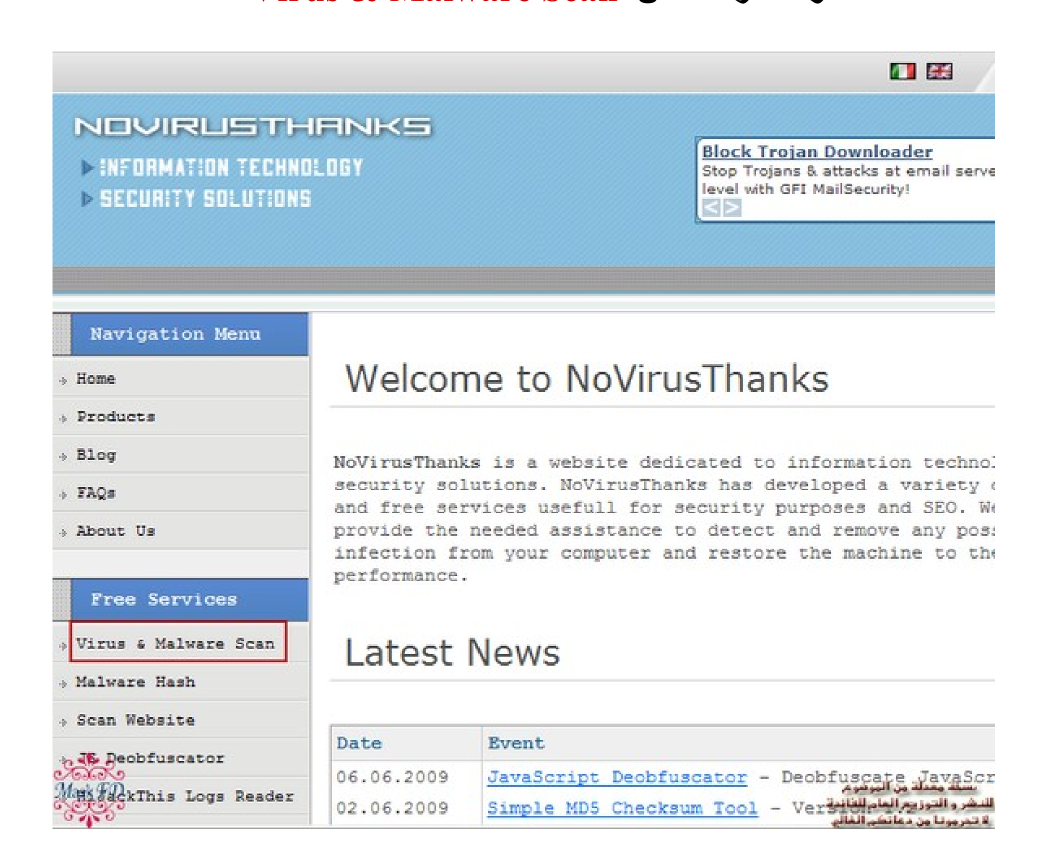
إذا شكيت في ملف بأنه فيروس لا تتردد برفعه على أحد هذه المواقع لفحصه و التأكد من سلامته .

www.virustotal.com
www.novirusthanks.com
http://virusscan.jotti.org/en

و هذا موقع يفحص رابط تحميل الملف .. جربته مع رابط للفور شيريد وكان تمام .. لكن ما أدري مع الرابيد شير و غيره كيف يكون .. ولا أدري ما هي آلية عمله .. تفضل و جرب ..

http://linkscanner.explabs.com/linkscanner/default.aspx

مثال على موقع NoVirusThanks
تفتح الصفحة الرئيسية .. و تروح على الخدمات المجانية Free Services
و تختار الفحص Virus & Malware Scan



من الأمر **استعراض Browse** تحدد موقع الملف على جهازك و تختاره ثم **موافق OK**

ثم تنقر على الأمر **Submit File**



في الصورة يقوم بالفحص .. إذا ما خلص اعمل تحديث للصفحة ..





إذا كان فيروس بتظهر لك مثل هذه النتيجة ..



File Information	
Report Generated:	3.7.2009 at 22.38.05 (GMT 1)
Time for scan:	38 seconds
File Name:	مجلدجديد.exe
File Size:	28 KB
MD5 Hash:	7965e07da5e55beb91436ccd5d27ddc9
SHA1 Hash:	73D239E80384B34B526915565947C0C1744D3D2B
Detection Rate:	13 on 24 (54.16%)



Antivirus	Sig version	Engine Version	Result
a-squared	03/07/2009	4.0.0.32	Trojan.Generic!IK
Avira AntiVir	7.1.4.175	8.1.2.12	Worm/VB.aol
Avast	090702-0	4.8.1229	Win32:AutoRun-AXF [Wrm]
AVG	270.13.2/2215	8.0.0.0	Worm/Generic.WDW
BitDefender	03/07/2009	7.0.0.2555	Trojan.Generic.1461382
ClamAV	03/07/2009	0.95.1	-
Comodo	1538	3.9	Unclassified Malware
Dr.Web	03/07/2009	5.0	-
Ewido	03/07/2009	4.0.0.2	-
F-PROT6	20090703	4.4.4.56	-
G-Data	19.6084	2.0.7309.847	Worm.Win32.VB.aol A
Ikarus T3	03/07/2009	1001044	Trojan.Generic
Kaspersky	03/07/2009	8.0.0.357	Worm.Win32.VB.aol
McAfee	02/07/2009	5.1.0.0	virus or variant W32/Generic.b
Malware Hash Registry	03/07/2009	N/A	-
NOD32 v3	4214	3.0.677	NewHeur_PE virus
Norman	2009/07/03	5.92.08	-
Panda	21/05/2009	9.5.1.00	Generic Malware
QuickHeal	03 July, 2009	10.0	-
Solo Antivirus	03/07/2009	8.0	-
Sophos	03/07/2009	4.32.0	Mal/SillyFDC-A



نصائح

بعض النصائح الناتجة عن تجربتي أو المستخلصة من خبرات أعضاء المنتدى الكرام

دائماً **احتفظ** بنسخة من ملفاتك الهامة على سيدي أو ديفيدي .. و**لا** أفضل نسخها فقط على فلاش أو هارديسك خارجي .. لأنها تكون بأمان أكثر من الفيروسات على سيدي أو ديفيدي حيث لا يمكن أن ينسخ الفيروس نفسه عليهم ..

أيضاً **احتفظ** ببرامج الحماية على سيدي أو بصيغة مضغوطة مثل ما نصح أخي الغالي **zezonasr** لأنها إذا أصيبت بالفيروسات لن تكون مفيدة .. و ستكون السبب في رجوعها ..

أنصح باستخدام برنامج لعمل نسخة احتياطية من النظام .. مثل **Acronis True Image2009**
لأنه يمكنك من استعادة نسخة من نظامك القديم بكامل برامجك القديمة بدون ما تضطر لتنصيب الويندوز و البرامج الأخرى ..طبعاً البرنامج يعمل الاستعادة من خارج الويندوز ..
و البرنامج أفضل بكثير من أداة استعادة النظام الموجودة في الويندوز ..
يمكنك تحميل كتاب عنه على هذا الرابط للأخ الكريم الغريب

DOWNLOAD

افحص جميع البرامج التي تقوم بتحميلها .. حتى الكتب الإلكترونية ذات الامتداد **EXE** .. لأنها جميعاً عرضة للإصابة بالفيروسات .. سواءً بقصد أو بدون قصد ..

أفضل **عدم** استخدام الكراكات المشبوهة .. و إذا أحببت استخدامها على الأقل قم بفحصها على موقع مثل **Virustotal** لتتأكد من نسبة خطورتها ..

و أكرر هنا قد **لا يعمل نظام ويندوز** لديك بعد الفحص لأن مكافح الفيروسات ممكن يحذف ملفات النظام المصابة بالفيروس .. لذلك لازم تنسخ ملفاتك الهامة قبل الفحص ..

تم بحمد الله و شكره و توفيقه.



إضافات الأعضـــــــاء

إضافات مميزة من الإخوة الأعضاء في موضوعي بالمنتدى .. حبيت تكتمل الفائدة بإضافتها .. بعضها قد أختصره لأخذ الفائدة منه فقط ..
مع جزيل الشكر لكل من شارك بالموضوع برد أو إضافة أو سؤال .

مشاركة مميزة من الأخ العزيز OUBID

وقد رأيت التنبيه على أمور نصحاً لإخواني وتتميما للفائدة:
1- الحرص على أقصى مستوى للحماية لأجهزتهم وذلك بـ : مضاد الفيروسات، الجدار الناري، الفلتر، تجنب المواقع التي يشير الفلتر أو الجدار إلى أنها مخترقة أو تحوي عناصر اختراق أو إشهارات ورسائل إلكترونية مفخخة.
2- تجنب تثبيت أكثر من انتي فيروس والحرص على التحديثات.
3- إذا أحسست بأن جهازك مصاب وأن الأنتي فيروس يكتشف الفيروس فينزعه ثم يعاود الرجوع فهذا يدل على تحرك الفيروس بين القرص الصلب و الذاكرة. والحل هنا أقراص الصيانة المزودة بأنتي فيروسات تعمل في DOS وأنا شخصيا أنصح بـ Avira rescue system خاصة إن حمّل من موقعه الأصلي واستعمل في ساعته فإنه يكون مزودا بأحدث التحديثات.

مشاركة مميزة من الأخ العزيز zezonasr

كانت لي تجربه سابقة مع فيروس W32/Sality.Y
عانيت منه كثيراً , قضيت أكثر من أسبوع لمحاولة التخلص منه , و بعد مرور الأسبوع و بالبحث و جدت أن الفيروس يزرع ملفين في القرص الصلب (C) لا أستطيع حذفهم أو فتحهم
حدث معي كل الآثار التي ذكرتها في موضوعك أعلاه
و علمت أنه لا توجد وسيله لحذف هذا الفيروس إلا بطريقه واحده :
قمت بتنزيل نسخة ويندوز جديدة , و قمت بالدخول للجهاز عن طريق الأمر Explore و كان لدى ملف مضغوط يحتوى على برنامج الأفيرا قمت بالضغط على البرنامج من داخله ثم قمت بتثبيت البرنامج ثم قمت بتحديثه و تركته ليفحص الجهاز
قام البرنامج بحذف جميع الألعاب و معظم البرامج لدى لإصابتها و بعد أن تأكدت أن الجهاز أصبح نظيف قمت بتثبيت نسخة ويندوز جديدة ثم أصبحت الأمور لدى كما كانت و أصبح الجهاز في حالته الطبيعية

و أنصح جميع إخوانى
بأن كل من يصيب جهازه فيروس سواء كان خطير أو لا
لا تدخل لجهازك بالشكل الطبيعي عن طريق الضغط على My Computer
ثم الضغط على الأقراص الصلبة مباشرة
و لكن استخدم الأمر Explore
بالضغط كليك يمين على الأقراص و الدخول للجهاز
أيضاً أرى أن ضغط البرامج يحميها من الإصابة بالفيروسات

مشاركة مميزة من الأخ العزيز أبو عبد العزيز 9

أريد أن أشير إليك بطريقة جميلة تستطيع من خلالها اكتشاف الفيروسات والتعامل معها وما تسببه من أضرار بالجهاز وتسهيل مهمة البحث عنها واكتشافها دون البحث عن أجهزة متضررة أو تتبع مشكلات الأعضاء والطريقة هي باستخدام برنامج

Microsoft Virtual PC

والبرنامج لا يخفى عليك بالتأكيد فهو يقوم بتنصيب أي نظام ترغب به في جهازك واستقطاع مساحة من الهاردسك والرامات خاصة به وتصفح كلا النظامين بجهازك مباشرة مع إمكانية النسخ واللصق من وإلى كلا النظامين مع بقاء كل نظام منعزل لوحده كل نظام له السستم الخاص به والريجستري الخاص به وما يحدث في نظام لا دخل للآخر به وبذلك تكون جمعت تجاربك في وقت قصير وتتأكد من تتبع الفيروسات بشكل دقيق حتى لو تضرر هذا النظام وتلف وانحذف بالكامل فإن نظامك الرئيسي ليس له علاقة بكل ذلك

احصل على البرنامج من مايكروسوفت من هنا

أحببت أن أضيف بعض النقاط والحلول:

1- قواعد بيانات برامج الحماية تختلف من برنامج لآخر لذلك لن نجد الكمال في أحدها لذا أنصح بتوفير بعض الأدوات جنباً إلى جنب مع برنامج الحماية لديك وهي كالتالي:

الأداة الأولى:

حماية الـ usb والمسماة بـ usb disk security

وهي أداة تحمي الجهاز من فيروسات الأقراص والفلاشات الخارجية

من هنا احصل على البرنامج مع تعريبه

الأداة الثانية:

geekz virus remover

وهي أداة تتميز بقاعدة بيانات قوية جداً تتميز عن كل برامج الحماية المعروفة والتي لم تتمكن من اكتشاف الكثير من الفيروسات الحديثة

من هنا أحصل على الأداة

الأداة الثالثة والأخيرة:

Malwarebytes' Anti-Malware

وهي أداة مهمتها اكتشاف البرامج الخبيثة بجهازك والكثير مما لا يكتشفه برنامج الحماية لديك

من هنا احصل على الأداة والشرح والتعريب

2- ليس شرطاً أن تشعر بخلل في جهازك حتى تعلم أنه مصاب ولكن يتطلب منك تنظيم استخدامك للجهاز والحرص على سلامته بتحديد وقت للفحص الشامل سواء من الفيروسات أو البرامج الخبيثة أو التروجونات فهناك أشياء تصيب أجهزتنا ولا نشعر بضررها إلا بعد وقت ليس بالقصير كذلك الحرص على تحديثه بشكل مستمر وفحص ما تقوم بتحميله من الانترنت مباشرة

3- هناك نقطة مهمة جداً جداً قد يغفل الكثير عنها وهي بعد القضاء على الفيروسات بعض

الفيروسات بعد أو عند القضاء عليها تقوم بتغيير بعض قيم الريجستري فتارة تجد بعضها تعطيك رسالة بحروف غير معروفة عند ظهور شاشة الترحيب أو قد تظهر لك رسائل بعد اقلاع الويندوز أو اختفاء بعض الأوامر مع العلم أنه تم التخلص من الفيروس فيبقى عليك الدور باصلاح الريجستري في جهازك والتأكد من سلامته باستخدام أحد برامج إصلاح الريجستري اخترت لكم هنا هذا البرنامج Registry Genius v3.1 وغيره من البرامج كثير

من هنا احصل على البرنامج

4- نقطة أخيرة بعض الفيروسات تقوم بعمل نسخة داخل مجلد ضمن مجلدات الــ temp لذا احرص بعد اصلاح مشكلتك بتنظيف مخلفاته سواء ملفات التمب أو الكوكيز أو مخلفات الذاكرة وأنصح باستخدام البرنامج الرائع :

cclener احصل عليه من هنا

مشاركة مميزة من الأخ العزيز bosaad

هذه أدوات مفيدة:

1- ComboFix

الشرح والتحميل

عطل برامج الحماية ثم حمل هذه الأداة ComboFix واحفظها على سطح المكتب

http://download.bleepingcomputer.com/sUBs/ComboFix.exe

أو

http://www.forospyware.com/sUBs/ComboFix.exe

عند تشغيلها بتظهر لك رسالة اضغط على Yes بعدها بتظهر لك رسالة ثانيه اضغط على Yes انتظر حتى تنتهي الأداة من فحص جهازك وبشكل تلقائي يعاد تشغيل جهازك وبعد إعادة التشغيل سوف تبدأ الأداة بالفحص مرة ثانية انتظر حتى يظهر لك تقرير ثم أغلق التقرير

يفضل استعمال جميع الأدوات من الوضع الآمن safe mode

Safe Mode طريقة الدخول إلى الوضع الآمن

2- FixIEDef

هنا الشرح والتحميل

FixIEDef اداة لحل اكثر المشاكل انتشارا مع الشرح

3- General_Removal

هنا الشرح والتحميل

أداة صغيرة الحجم كبيرة المفعول

بالنسبة لتوضيح نقطة إيقاف استعادة النظام .. تم رفعه بالموضوع لإتمام الفائدة .

مشاركة مميزة من الأخ العزيز slammer

تنقسم أنواع الملفات الضارة إلى عدة أنواع (بينما الناس يطلقون عليها جميعاً اسم فيروس) و لكل نوع مواصفاته و مدى قدرته على التخريب.

1- الفيروس Virus

و هو برنامج عادي له وظيفة معينة يقوم بتأديتها حسب مهارة من قام ببرمجته .. فبعضها قد يعمل على إتلاف الملفات والآخر يقوم بحذفها ... و هكذا. و من أهم صفات الفيروس أنه لا يبدأ عمله إلا بسبب مستخدم الجهاز نفسه ... فقد يقوم بتشغيله بدون علمه و لكن يبقى هو من تسبب في ذلك .

2- الدودة Worm

هذه البرامج أقل ضرراً و خطورةً من الفيروسات و هي لا تعمل على إحداث أضرار بليغة و يتركز وجودها في الذاكرة المؤقتة RAM فلو أغلقنا الجهاز سوف تمحى تلك البرامج من الذاكرة.
و يهدف مبرمج هذه البرامج إلى تقليل فعالية النظام لأن الدودة تعمل على نسخ نفسها في الذاكرة بشكل لا متناهٍ مما يسبب البطء .

3- حصان طروادة Trojan Horse

تصمم هذه البرامج لسرقة معلومات معينة من جهاز الضحية و قد تكون معلومات حساسة و مهمة كأرقام الحسابات البنكية أو الصور الشخصية و الحماية منها تتم عن طريق الجدار الناري و ليس مضاد الفيروسات .

4- الثغرات الأمنية Back Door

ممرات خفية في جهاز الضحية يعمل من خلالها الشخص المخترق إلى الوصول إلى داخل الجهاز للتجسس عليه و قد يكون سبب هذه الثغرات ضعف برمجي في أحد البرامج أو نقص كفاءة برامج الحماية نتيجة عدم التحديث.

5- القنابل البرمجية Logical Bomb

و هذه البرامج تم برمجتها لتقوم بعمل معين في لحظة معينة. تختلف هذه اللحظة حسب البرمجة (فقد تكون تاريخ معين أو فتح برنامج معين ... الخ) و تختلف خطورتها حسب مهارة من قام ببرمجتها. يمكن يبرمجها موظف مفنشينه و يخليها تشتغل بعد ما يطلع من الشركة ... خخخخ

6- الملفات الدعائية Spam

غالباً لا تكون ضارة بالجهاز و لكنها مزعجة للمستخدم و يمكن التخلص منها باستخدام البرامج المخصصة لهذا الغرض.

7- الرسائل الخادعة Hoaxes

أيضا ليست ضارة في ذاتها و لكنها تحمل معلومات مضللة و غير صحيحة .... و منها ما يكتبه البعض من الرسائل المنتشرة في الانترنت ... "أين أنتم يا مسلمين ....الخ الخ الخ" و قد تدخل لذلك الرابط فتجد أن العملية ليست سوى خدعة و المطلوب هو الدعاية لموقع أو منتج معين.

مشاركة مميزة من الأخ العزيز alimaj

نصيحتي وهي حسب تجربتي على مدى 3 سنوات من استخدام المكافحات
لا تشتري مكافح أو تستخدم سيريال أنا احمل نسخ الـ 30 يوم وفيها جميع المزايات والمكافح ماشي معاي 100% وإذا انتهى راح أحمل مكافح آخر ستعرفون السبب بطبيعة الحال العملية كلها لعب في الريجيستري .
إذا لم تنجح في حذف المضاد 100% لازم تستعمل أداة الشركة الخاصة بحذفها
وأنا استخدم هذه الطريقة
- قوقل
- اكتب مثلا avira uninstall tool
- أحمل
- أزيل المضاد
- أركب مضاد اخر
ونفس الحكاية كل 30 يوم

مشاركة مميزة من الأخ العزيز deferentman
مفيدة لو كان جهازك بطيء مع مكافح الفيروسات ..
عندي ملاحظة بسيطة وهي اقتراح طبعاً ذكرت أنه يمكن استخدام الإصدار الشامل Security لكن توجد مشكلة وهي أن الإصدار الشامل للمكافح تكون نسخته ثقيلة على الجهاز في حالة ويندوز فيستا يكفي استخدام إصدار الانتي فيروس مع جدار الحماية في فيستا فذلك فعّال جداً ونفس الحال مع الاكس بي

مشاركة مميزة من الأخ العزيز سلطان العبدلي
أوردت رأي الأخ الكريم بخصوص ظهور مجلد RECYCLE.BIN$ لكني أعتقد إن الفيروسات لا تظهر الملفات المخفية بل تخفيها لأنها بالأساس مخفية لكني افتح باب للرأي الآخر ليأخذ حقه وخاصة إن صاحب الرأي الأخ العزيز سلطان
لي بعض الملاحظات :
zhengbo وبجانبه ملف AUTORUN ليس فيروس بل هو مجلد يقوم بإنشائه أحد برامج حماية الفلاش ليمنع فيروس الاتورن من نسخ نفسه إلى الأقراص
ومن الصدف أن الأخ العزيز أبوعبدالعزيز 9 وضعه في رده وهو أول برنامج في رده
رابط البرنامج هنا
http://www.absba.org/showthread.php?t=754556

وعن نفسي استغنيت عنه واستبدلته بهذا البرنامج المميز لحماية الفلاش
لازاله فيروس الاوتورن وحمايه الجهاز من فيروسات الفلاشه Autorun Virus Remover 2.3 0702

بالنسبة لظهور مجلد $RECYCLE.BIN
فاحب اقولك ان ظهور مجلد $RECYCLE.BIN على القرص هو فيروس لان مجلد الـ $RECYCLE.BIN لايظهر لوحده حتى لو كنت عامل إظهار للملفات المخفية إلا لو كان بسبب فيروس وحله هنا:
14-3-2009 اداه FixIEDef 1.7.22.7514 لازاله الفيروسات

بالنسبة لفيروس W32/Sality هنا أداتين من المبدع صفوان الرضمي
هذه بعض الأدوات الخاصة بحذف هذا الفيروس Virus.Win32.Sality
1- أداة من شركة الكاسبر ضد الفيروس برابط مباشر
http://support.kaspersky.com/downloads/utils/sality_off.rar
2- أداة من شركة AVG برابط مباشر
http://www.avg.com/filedir/util/avg_rem_sup.dir/rmsality/rmslt.exe

وهذه اداه من رفعي:
W32.Perlovga.Remover
http://www.files2net.com/files/17351...ga.Remover.zip

أداة تنظيف ريجستري الافيرا متوفرة في موقعه الرسمي
http://www.avira.com/en/support/support_downloads.html
Avira AntiVir RegistryCleaner
وهذا رابطها المباشر
http://dl1.pro.antivir.de/down/windows/registrycleaner_en.zip

مشاركة مميزة من الأخ العزيز الهترك
مجلد System Volume Information هو مجلد يتم تخزين نقاط الاستعادة به وهو من مجلدات النظام كما أسلفت وعادةً تحفظ به نسخ من ملفات النظام بتواريخ مختلفة بما فيها الملفات المصابة بالفيروسات إذا كانت هناك إصابة... ولذا تعود الإصابة عند استعادة النظام ..
ويختفي المجلد تماما لوعطلنا خاصية استعادة النظام ... يختفي بكل ما بداخلة.
لذا عند فحص ومعالجة جهاز تم التأكد من إصابته يفضل تعطيل الخاصية .... ثم تفعيلها مرة أخرى بعد تمام المعالجة..

خاتمـــة



خاتمة الموضوع

هذا الجهد المتواضع و المليء بالقصور إهداء لكل المسلمين .. أتمنى يفيدكم و يعينكم بعد الله على التخلص من الفيروسات و فهم آليات عملها .

ما هو واجبك تجاه الموضوع

الموضوع كتب للفائدة العامة .. و كنت أتمنى نشره و توزيعه بصورة كبيرة .. لكني لأسف لم أتمكن من ذلك ..
لذلك واجبك أخي الكريم أختي الكريمة أن توزعوه لمن يحتاجه .. لأنه من نشر العلم و كتمه إثم و مضرة عامة .. حيث أن هدف الموضوع هو حماية أجهزتنا من الفيروسات .

و طلب صغير

وهو عند الله كبير .. دعاء بظهر الغيب لكاتب الموضوع .. يعلم الله كم أخذ هذا الموضوع من وقتي و كم بذلت في ترتيبه و تنسيقه و تصميمه لإيصاله لكم بهذه الصورة المتواضعة ..
فلا تحرموني من دعائكم الطيب بظهر الغيب و والدي و أهلي و أقاربي و المسلمين بالمغفرة و الهداية و الرحمة و الرزق الحلال المبارك و دعاء خاص لوالدتي بالشفاء العاجل .. و أسأل الله العظيم الكريم لكم أضعاف ذلك .

للتواصل

لمن يريد التواصل معي يمكنه مراسلتي على هذا الإيميل .. لكني لا أعدكم بشيء لأني مشغول جداً هذه الفترة من حياتي ..
Maskfd77@hotmail.com

بارك الله فيكم و وفقكم لما يحبه و يرضاه .

نصيحة بعنوان (لا تنسَ)

نصيحة بعنوان لا تنسَ (تكتب بدون ى) لكل الإخوة و الأخوات المسلمين و المسلمات ..
أرجو أن تدخل قلوبكم وعقولكم .

لا تنسَ بر والديك واعطف عليهما واخفض جناحك لهما .. فهو واجب عليك وهو أقل ما يستحقون تجاه تعبهم عليك في صغرك (حتى ولو صدر تقصير منهم) فعظيم حقهم عليك أكبر من حقير حقك عليهم
لا تنسَ سهرهم عليك في مرضك وتعبهم واجتهادهم لتوفير ما يرضيك ويريحك
لا تنسَ أنك أملهم وحلمهم في تحقيق ما عجزوا عنه .. فلا تكن خيبة أمل لهم
لا تنسَ برهم بعد مماتهم بالدعاء والاستغفار لهم وبر صديقهم
لا تنسَ واجباتك الدينية وأهمها الصلاة والزكاة والصوم
لا تنسَ قدرة الله عليك وعظم عذابه ونقمته كما لا تنسَ سعة رحمته وكريم عفوه
لا تنسَ ذكر الله تعالى في كل وقت وحين والصلاة والسلام على رسوله الكريم محمد صلّ الله عليه وآله وصحبه وسلم
لا تنسَ عذاب النار لتترك حب الدنيا والمعاصي و لا تنسَ نعيم الجنة لتقبل على الآخرة والطاعات
لا تنسَ أن باب التوبة مفتوح لك إلا إذا حان أجلك أو قامت الساعة .. فبادر إلى التوبة
لا تنسَ الفقير المعدم من الزكاة والصدقة والدعاء والوجه البشوش
لا تنسَ المريض العاجز من العيادة والزيارة والتفاؤل أمامه بالشفاء العاجل ولا تقنطه من رحمة الله .. و لا تنسَ المريض الفقير بالمساعدة بعلاجه
لا تنسَ جارك من السؤال عن حاله ومساعدته والتبسم له
لا تنسَ إبداء النصيحة بالأسلوب الحسن والكلمة الطيبة فتكون ليناً في أمرك بالمعروف ونهيك عن المنكر وتذكر بأن حسن تعاملك قد يهدي المخطئ للصواب وأن غلظتك عليه قد تزيده ضلالاً
لا تنسَ أن كتم العلم فيه إثم كبير .. فلا تبخل على إخوانك بما فتح الله عليك
لا تنسَ الصبر والحلم على من أخطأ بحقك واعتدى عليك
لا تنسَ خفض جناحك و تلطفك مع من هم دونك .. أهلك وعاملك وخادمتك وغيرهم .. وتذكر بأن الراحمون هم من يرحمهم الرحمن وليس قساة القلب الظالمين
لا تنسَ أن طهارة القلب أهم من كثرة العمل الصالح .. فكم من حسنات تكسبها يضيعها فساد القلب بالتكبر على العباد أو الحقد أو الحسد أو الغيبة أو غيرها من أمراض القلوب
لا تنسَ أن الكبرياء لله وحده فقط .. وأنك ضعيف قليل الحلية .. وأن من أعطاك قادر على حرمانك
لا تنسَ إخوانك المجاهدين في كل مكان .. في فلسطين و العراق و أفغانستان و كل مكان
لا تنسَ مساعدتهم ليس فقط بالمال ولكن بالدعاء الصادق المخلص فيه
لا تنسَ أن تحمد الله تعالى دائماً على نعمه العظام وأهمها أن أكرمك بالإسلام .. ولا تقدم عليه فخراً أنك من قبيلة أو دولة فكلها إذا لم تكن مسلماً لا تنفعك بشيء يوم الحساب
لا تنسَ أن الدعاء بظهر الغيب لأخيك المسلم يرجع عليك وعليه بالفائدة .. فلا تحرم نفسك منه .

اللهم اغفر للمسلمين و المسلمات و المؤمنين و المؤمنات الأحياء منهم و الأموات
اللهم صلّ و سلم و بارك و أكرم و أنعم على عبدك و حبيبك و رسولك سيدنا محمد النبي الأمي و على آله و صحبه و التابعين لهم بإحسان إلى يوم الدين
سبحان ربك رب العزة عما يصفون و سلام على المرسلين و الحمد لله رب العالمين